# Impact of Common Cause Failure on Reliability Performance of Redundant Safety Related Systems Subject to Process Demand

Siamak Alizadeh [a] , Srinivas Sriramula [b]

School of Engineering, University of Aberdeen, AB24 3UE, Aberdeen, UK.

[a] Email Address: Siamak.Alizadeh@hotmail.co.uk; Tel: +44 (0)7726 295920.

[b] Corresponding Author: Dr Srinivas Sriramula; Email Address: s.sriramula@abdn.ac.uk; Tel: +44 (0)1224 272778.

# Abstract

Common Cause Failures (CCFs) can compromise reliability performance of safety related systems and hence configurations with identical redundant units receive special attention in many industries, including in automotive, aviation and process applications. This paper introduces a new reliability model for redundant safety related systems using Markov analysis technique. The proposed model entails process demand in conjunction with CCF and established system failure modes such as dangerous undetected failures for the first time and evaluates their impact on the reliability performance of the system. The reliability of the safety related systems is measured using the Probability of Failure on Demand (PFD) for low demand systems. The safety performance of the system is also appraised using Hazardous Event Frequency (HEF) to quantify the frequency of system entering a hazardous state that will lead to an accident if the situation is not controlled accordingly. The accuracy of the proposed Markov model is verified for a case study of flammable liquid storage tank overpressure protection system. It is demonstrated that the proposed approach provides sufficiently robust results for all demand rates, demand durations, dangerous undetected and CCF frequencies and associated repair rates for redundant safety related systems utilised in low demand mode of operation.


**Keywords:** Markov chains; safety instrumented systems; safety related systems, common cause failure; process demand; hazardous event frequency.


# 1.0 Introduction

In addition to quality, productivity and profitability, safety assessment is nowadays an integral part of the functional safety strategy of companies. In this regard the first step for minimising the level of risk is awareness and understanding the concept of hazard and layers of protection. A diverse range of Independent Protection Layers (IPL) is increasingly used by the operators to protect from undesirable events. The IPLs can be applied in the form of administrative procedures or by physical barriers such as mechanical systems, and instrumented protective functions. The sequence of IPLs presented by the “onion model” [1, 2] starts from the centre and proceeds outwards, first with layers contributing towards reducing frequency of hazardous events and then with layers mitigating consequences of accidents [3]. An Electrical, Electronic and

Programmable Electronic System (E/E/PES) such as a Safety Instrumented System (SIS) can be used as an IPL in both capacities. Its goal is to provide protective functions by detecting abnormal conditions, performing the required safety action and maintaining the safe status of the system.

The international standard IEC 61508 [4] can now be considered as the primary standard for the specification and the design validation, and verification of the safety function realised by an E/E/PES safety related system throughout all phases of its lifecycle. Its introduction in 1998 [4] has induced many companies to understand the new concepts in evaluation and the influence of all parameters in the SIS performance assessment. The principles introduced in the generic standard are also adapted for specific applications, such as IEC 61511 [1] for the process industry, IEC 62425 [5] for the railway industry, and ISO/DIS 26262 [6] for the automobile industry. The sectorial variation for the international standard for the process industry, IEC 61511 [1], is intended for the practicing engineers and users of safety instrumented systems in upstream and downstream process industries.

It is essential to analyse the sequence of IPL activation in the reliability performance quantification. Where a SIS is the last layer of protection utilised to mitigate the consequences of a hazardous event, then the failure of SIS may directly lead to an accident. IEC 61508 [4] stipulates that the performance of a SIS shall be proven using a suitable technique. This performance is the unavailability of the SIS to fulfil the required safety function and its confidence which is defined by the well-known Safety Integrity Level (SIL) [7] via computation of probabilistic parameters recognised as Probability of Failure on Demand (PFD). Some of the modelling techniques are cited in the appendices of international standards, although no specific approach is proposed. The most frequently used techniques to analyse the reliability of SIS include Simplified Equation (SE) [4, 8], Bayesian methods [9], Reliability Block Diagram (RBD) [10, 11], Fault Tree Analysis (FTA) [12, 13], Markov Analysis (MA) [14–16] and Petri Nets (PN) [7]. These diverse techniques have their own advantages and limitations. Each of these techniques may cover several aspects of the system behaviour concerning safety. Although individual aspects of the system's risk related behaviour may be thoroughly analysed by some of the techniques, they do not always lead to identical results.

Rouvroye and Brombacher [17] carried out a thorough comparison of reliability modelling techniques and established that Markov chain based reliability analysis covers most aspects for quantitative safety evaluation. Additionally, the performance of different reliability modelling techniques explored by Innal [18] concluded that Markov methods are the most suitable approach predominantly due to their flexibility. Guo and Yang [10] also emphasised that Markov analysis evinces more flexibility in contrast to other reliability modelling tools and is the only technique that can describe different states of a system and the dynamic transitions amongst these states. In recent years, several Markov models were developed that integrate the dynamic behaviour of SIS and the effect of demand inflicted on the safety instrumented system. A simple Markov chain of SIS subject to demand was first presented by Bukowski [15] which comprised of both dangerous detected and undetected failures. The preliminary model of Bukowski [15] was further elaborated by Jin et al. [3], incorporating the repair rate of dangerous undetected failures for safety instrumented system in conjunction with inclusion of safe failure and associated repair rate. In discrete attempts, Liu et al. [19], and, Alizadeh and Sriramula [20] extended the boundaries of Markov analysis and produced transition diagrams for a redundant configuration, however the impact of common cause failures were overlooked by exclusion. In this paper we intend to resolve the limitation of the model introduced by Liu et al. [19] by embedding CCFs in conjunction with established component failures for redundant configurations subject to demand. Therefore, this model is considered as one step closer to evaluating authentic behaviour of the redundant configurations since CCFs influence reliability and safety performance of the safety related systems and cannot be omitted in generic or specific case SRS architectures.

The primary objective of this paper is to propose an exclusive Markov model to evaluate the reliability performance of redundant Safety Related Systems (SRSs) subject to demand which combines the effect of both dangerous undetected and common cause failures. The model introduced by Liu et al. [19] is developed further by using Markov chains for their ability to model accurately and correctly redundant safety related systems in low demand. The newly introduced reliability model is flexible to accommodate diverse repair strategies of redundant configurations. The multiple stage repair strategy of CCF for redundant safety systems has been studied by Alizadeh and Sriramula [21] whereas in this paper, an alternative strategy comprising single stage repair of CCF for redundant SRSs is considered. The proposed new model also

incorporates the following parameters: dangerous undetected failures, common cause failure and repair rates, demand rate and demand reset rate but assumes the absence of automatic diagnostics and proof test coverage. In the next Section the basics of safety instrumented systems are presented. In Section 3 we recall the mathematical preliminaries and fundamental elements of reliability modelling. Section 4 is devoted to the Markov models of simple and redundant safety related systems followed by a numerical analysis presented in Section 5. Applications of the proposed model are also discussed in Section 5 based on the results obtained, and concluding remarks are outlined at the end of this section.

# 2.0 Safety Instrumented Systems

## 2.1 Overview

The primary objective of a SIS is to bring the equipment it oversees in a safe position when the Equipment Under Control (EUC) deviates from its design intent and results in an unwanted consequence (e.g. loss of containment leading to explosion, fire, etc.). SISs are widely used to prevent occurrence of hazardous events, and/or to mitigate their undesirable consequences to humans, the environment and financial assets.

A SIS is functionally split into three main subsystems: (1) a Sensor Element (SE) to detect abnormal situations; (2) a Logic Solver (LS) to process and initiate an executive action based on a predefined logic and; (3) a Final Element (FE) to respond to the detected abnormal situation [4]. Redundant configurations are often used to enhance the reliability of SISs, hence each subsystem may consist of one or more (usually but not always) identical channels. In this regard, a SIS (or SIS subsystem) is known to have a *k*oo*n* configuration when *k* components of its total *n* components must operate to provide the required system function. Classic SIS configurations consist of 1oo1, 1oo2, 1oo3, and 2oo3 architectures [18]. In this article, only the two first configurations are studied, a 1oo1 system and a 1oo2 redundant configuration. This is because we believe that the main features of our new model will be demonstrated by these simple systems with reasonable amount of nodes and volume of the transitions, in comparison to configurations with higher level of redundancies. Furthermore, the aforementioned systems have been thoroughly assessed with other approaches [4, 21] therefore enabling comparison.

It is worth noting that a SIS may perform more than one Safety Instrumented Function (SIF) to achieve a safe state for the EUC including the system the SIS is protecting against a specific process demand [11]. The reliability analysis is always conducted with respect to one specific SIF, as it is the SIF that provides protective function against a specific hazardous scenario. Nevertheless, majority of publications in the literature refer to reliability of SIS, and we use this expression consistently even though what we essentially refer to is one SIF. In this article, the reliability modelling is presented for a single subsystem of identical elements, but it is relatively effortless to extend the computation to the entire SIF.

## 2.2 Demand Modes

IEC 61508 / 61511 distinguish between SISs in low demand, high demand and continuous mode of operations, where the borderline between low demand and high / continuous demand mode is the demand rate of once per year. This distinction is made based on two criteria consisting of the frequency at which the SIS is anticipated to operate in response to demands, and the expected time interval that a failure may remain undetected, considering the frequency of proof test. IEC 61511 [1] distinguishes between two modes of operation namely demanded mode and continuous mode. SISs operating in demanded mode are mainly reactive barriers, whereas SIFs operating in continuous mode are mainly considered as proactive barriers [23], see Figure 1. Most attention in the process industry has been paid towards demanded SIFs and in specific SIFs in low demand mode. This is reflected in the available publications where the vast majority investigated reliability of low demand SIFs [3,6,11,16,19,24–28]. The international standards also focus predominantly on demanded SIFs with the main focus on the low demand mode of operation.

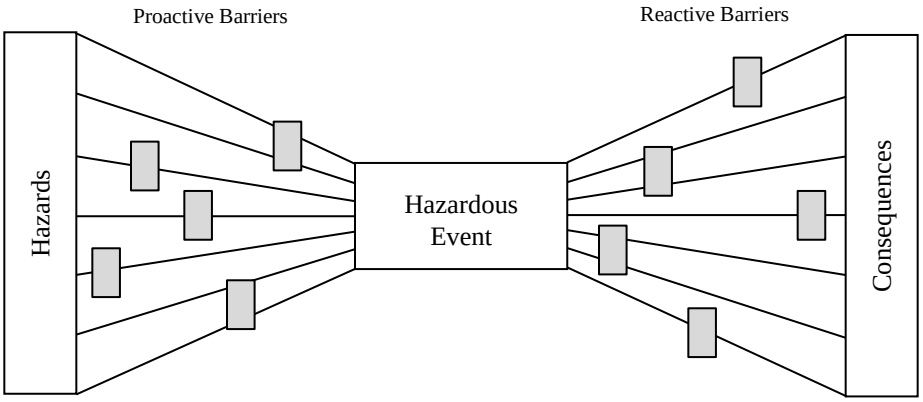


Figure 1 – Bowtie Diagram with Proactive & Reactive Safety Barriers for Hazardous Events

The demand rate for a SIS may fluctuate from infrequent to continuous and the duration of each demand may vary from instantaneous up to a relatively lengthy period (e.g. hours). High demand systems are different from low demand systems, and the same analytical evaluation techniques cannot be implemented for all systems in different modes of operations. Techniques based on RBD and FTA are generally not appropriate for assessment of high demand SISs when the duration of demands is also substantial. Several authors have indicated that Markov methods are best suited for analysing SISs operational in both high and low demand systems [19].

Despite the seemingly clear split between the low demand and high demand mode of operations, there are still some underlying issues that result in confusion and complications in the quantification of SIS reliability performance [3]:

(1) neither in IEC 61508 nor in or any other reliable sources the rationale behind using once per year or twice the frequency of functional tests as the borderline is fully justified [25].

(2) the various elements may have different demand rates for some SISs. It is not uncommon that parts of the logic solver may, be commonly used between various SIFs and hence can be operated more often than the initiator and/or final elements, making it difficult to determine the exact mode of operation.

(3) the demand mode classification discards the criticality of demand duration. In some rare applications, once the demand takes place, it may generate "sub-demands" during an extended period of time. The SIS may therefore be in the low demand mode between demands, and in the high demand mode while responding to the demand due to its duration. A classic example of SISs in these applications is a Blow-Out Preventer (BOP) that is employed to stop uncontrolled flow from oil and gas wells during drilling. Situations that require full closure of the BOP are very infrequent, however when the BOP is activated, it must be able to withstand the full well pressure for hours or even weeks.

Neither the demand mode classification nor the proposed reliability performance measures for low and high demand systems, can resolve these issues. As such, rather than establishing a clear borderline between different modes of operation, some authors suggest to incorporate the rate of demands into the analysis by using Markov modelling [13, 24, 28].

## 2.3 Failure on Demand & Integrity Levels

The basis of the international standards IEC 61508 / 61511 is the establishment of the safety lifecycle and the introduction of Safety Integrity Level (SIL). The standard stipulates that every safety function shall achieve a specific SIL, determined based on a suitable risk assessment. The SIL is a quantitative index that specifies the acceptable probability of dangerous failure that a SIS can retain to be considered as an appropriate IPL for a given safety integrity requirement. Distinction is made in SIL criteria between two different types of operations, the average Probability of Failure on Demand (PFD) for low demand mode of operations and the Probability of Failure per Hour (PFH) for high demand systems. The aim of PFD and PFH is to maintain the residual risk at an acceptable level [30]. The IEC 61508 standard [4] outlines four classifications of integrity levels based on the PFD and/or PFH as shown in Table 1 where SIL 4 corresponds to the highest and SIL 1 to the lowest integrity level requirements:

Table 1 – Definition of SIL Levels

| **SIL** | **1** | **2** | **3** | **4** |
|---|---|---|---|---|
| $PFD$ | $[10^{-2}, 10^{-1})$ | $[10^{-3}, 10^{-2})$ | $[10^{-4}, 10^{-3})$ | $[10^{-5}, 10^{-4})$ |
| $PFH$ | $[10^{-6}, 10^{-5})$ | $[10^{-7}, 10^{-6})$ | $[10^{-8}, 10^{-7})$ | $[10^{-9}, 10^{-8})$ |

The SIS design entails achievement of minimum levels of safety integrity as necessitated by the standard. The safety integrity requirements include the restriction of the system PFD to a maximum target limit in conjunction with the compliance with minimum levels of Hardware Fault Tolerance (HFT). Therefore, in addition to the requirement of PFD, the highest SIL that can be claimed for a subsystem's combination of hardware is limited by architectural constraints, which are detailed in IEC 61508. The overall value of average probability of failure on demand of a SIS ($PFD_{SIS}$) is calculated using the PFD values of one or more of input elements, logic solvers and final elements [28, 30], therefore the weak link prevails in all cases as follows:

$$PFD_{SIS} = \sum PFD_{SE} + \sum PFD_{LS} + \sum PFD_{FE} \quad (1)$$

The context of PFD and PFH is studied by various authors and a common measure for use with both demand modes (low and high) is recommended. This includes incorporation of the rate of

demands into the analysis [13, 15, 24] instead of drawing a clear borderline between low and high demand mode of operation. Misumi and Sato [13] utilise fault tree analysis technique to develop analytical formulas for a newly introduced "hazardous event frequency", whereas Bukowski [15] computes the probability of being in a state of "fail dangerous and process requires shutdown" (PFDPRS) based on a Markov chain. Although these proposals are promising in quantification of SIS reliability performance in general, further development is needed to reflect all pertinent modelling aspects. In this paper we use both the PFD and Hazardous Event Frequency (HEF) as performance indicators of the reliability model proposed for redundant safety related systems subject to demand mode.

# 3.0 Modelling Fundamentals

## 3.1 Component Failure Modes

Safety instrumented systems are exposed to two main types of failures; those that prevent the execution of the SIF, normally referred to as dangerous failure, and those that do not, which are called safe failures [4]. Dangerous failures represented by $\lambda_D$ are characterised as failures which cause the system to fail dangerous, e.g. the component does not operate on demand. Safe failures denoted by $\lambda_S$ are characterised by a spurious alarm or trip which causes the system to fail safe, e.g. the component operates without demand [32]. Spurious activations should be avoided during SIS design, and if a spurious activation occurs, it should bring the EUC to a safe state and maintain accordingly. Safe failures do not have any effect on the ability of the SIS to perform its functions.

The overall failure rate of a component $\lambda$ is obtained by $\lambda = \lambda_D + \lambda_S$. In this paper both safe and dangerous failures are included within the proposed reliability models of safety instrumented systems. Each of these two categories is further split into detected failures and undetected failures. Detected failures are revealed by diagnostic testing, whereas undetected failures are only revealed by proof testing or during the solicitation by the EUC. Dividing the dangerous and safe failures into detected and undetected, four distinct failures can be distinguished. These failure modes comprised of Dangerous Detected (DD), Dangerous Undetected (DU), Safe

Detected (SD) and Safe Undetected (SU). The overall component failure rate consists of the summation of these four main elements:

$$\lambda = \lambda_{DD} + \lambda_{DU} + \lambda_{SD} + \lambda_{SU} \quad (2)$$

where $\lambda_{DD}$ represents DD failure rate, $\lambda_{DU}$ is DU failure rate, $\lambda_{SU}$ denotes SU failure rate and $\lambda_{SD}$ signifies the SD failure rate. In order to model SIS reliability, it is vital to recognise the nature of the failure modes and means of their detection. This would allow the development of appropriate strategies to ensure the required functionality, reliability and availability of safety instrumented functions are retained as specified in accordance with IEC 61508 [4].

## 3.2 Testing Strategies & Failure Detection

A SIS is an active IPL system that is triggered only when a demand is inflicted. Failures may therefore occur and remain hidden until the system is demanded or tested. Here, we briefly mention the two main categories of testing strategies for detection of failures.

### 3.2.1 Diagnostic Testing

Diagnostic testing can detect the dangerous failures without fully discharging the main function of the safety instrumented system and interrupting the EUC. For instance, the diagnostic testing may reveal drifting in the signal conversion of a transmitter without activating the instrument device. Diagnostic testing is provided from time to time by the manufacturer as a feature of programmable electronic components. The interval between consecutive diagnostic tests is called diagnostic test interval which is usually short, ranging from milliseconds to hours in extreme scenarios. This allows sufficient time to execute repair activities for low demand SISs and restore the component function prior to the next demand.

The fraction of dangerous failures that can be detected by diagnostic tests is known as Diagnostic Coverage (DC) [4]. The DC can be estimated using a Failure Mode & Effect Analysis (FMEA) at the component level [32, 33]. The possible failures are then sought to determine if they can be detected by diagnostic testing. It is seldom evaluated whether such a testing leads to side-effects

[26]. The ratio of the detected dangerous failure to the total dangerous failures (detected and not detected) is defined by IEC 61508 as the DC rate and computed as [16]:

$$DC = \frac{\lambda_{DD}}{\lambda_D} = \frac{\lambda_{DD}}{\lambda_{DD} + \lambda_{DU}} \tag{3}$$

The DC rate in Equation (3) characterises the effectiveness of the diagnostic testing. Although the diagnostic testing can reveal dangerous failure almost immediately when failure occurs, only a fraction of dangerous failures can be detected. This fraction of dangerous failures is recognised as DD failures, and the remaining failures are defined as DU failures which are only detected by proof testing. Hence, DC rate divides the dangerous and safe failures into detected and undetected, resulting in four discrete failure modes [35] as follows:

$$\begin{aligned} \lambda_{DD} &= DC.\lambda_D & \lambda_{DU} &= (1 - DC).\lambda_D \\ \lambda_{SD} &= DC.\lambda_S & \lambda_{SU} &= (1 - DC).\lambda_S \end{aligned} \tag{4}$$

The total failure rate now can be revised as the following equation considering the estimated DC:

$$\lambda = DC.\lambda_D + (1 - DC).\lambda_D + DC.\lambda_S + (1 - DC).\lambda_S \tag{5}$$

Dangerous detected failures are often ignored in reliability analysis of safety instrumented systems since it is assumed that when a DD failure occurs, the EUC is brought to a safe state instantaneously. This assumption is not always fulfilled as the diagnostic test interval is not negligible always, meaning that a DD failure may not be detected immediately after its occurrence. Furthermore, switching to a safe state may not be feasible promptly after a revealed dangerous failure. The operational philosophy may sometimes allow the SIS to operate in a degraded mode [36]. The proposed reliability model in this paper is focused on DU failures and evaluates their impact on the performance of redundant safety instrumented systems.

### 3.2.2 Proof Testing

Since the diagnostic testing is unable to detect all dangerous failures, proof tests are performed periodically to reveal the latent failures which prevent the SIS to fulfil its safety function if it is solicited. The proof test also facilitates evaluation of SIS performance and whether it reaches and preserves its allocated safety integrity level [37]. Thus, these tests are vitally important for the SIS as they enable operators to maintain and improve the safety integrity level without making design modifications [37]. Proof tests are in many cases performed at regular time intervals, although the frequency of such tests is considerably lower than for diagnostic tests and it may vary from months, up to years. Proof test duration is an important parameter for calculating the reliability of SIS. For safety instrumented systems operating in low demand modes, it is essential to perform proof testing to avoid a DU failure remaining hidden for a prolonged period of time. The necessity and value of proof testing for improving the reliability of a high demand SIS however is not always evident, as the likelihood of revealing a failure before a demand occurs is reduced.

In many reliability analyses, the proof test is assumed to reveal all failures. This means that all the undetected failures can be detected and repaired; otherwise, undetected failures will be discovered with a certain probability and rectified upon detection of DU failures in a comprehensive system overhaul before a demand occurs. Perfect proof testing in practice is difficult to achieve even for a moderately complex SIS. There may be certain failures that remain hidden until a major overhaul, a real demand, or the end of the SIS lifetime. In this paper we assume that a thorough examination is carried out during the proof tests. Therefore, these tests are perfect in detection of the latent failures (100% success rate) and the system can be restored to “as good as new” condition or as close as possible to this circumstance [38]. A proof test may lead to partial process disturbance and hence it is associated with certain economic expenditure in addition to the cost of labour, materials and equipment required for completion of the testing.

## 3.3 Common Cause Failures

IEC 61508 pointed out the presence of CCFs for redundant configurations which can occur in channels following the same cause [21, 38]. The importance of CCFs in SIS performance

assessment is also documented in many papers e.g. Hokstad et al. [40] and Lundteigen et al. [31]. A CCF is a failure affecting several or all of the redundant components of a SIS simultaneously, leading to impairment of the safety function and ultimately SIS failure in response to a process demand. Consequently, CCFs must be identified during the design phase and their potential impact on the SIS functionality must be analysed and eradicated or reduced as far as reasonably practicable [30, 39].

The introduction of the common cause expression in reliability analysis affords the opportunity for evaluation of CCF and its impact on the failure probability of a SIS [35, 36]. In this regard, the PFD can be calculated taking cognisance of such CCFs by directly incorporating them into the SIS reliability model [41]. The computing parameters of CCF are usually evaluated using feedback data. However, considering the challenge in obtaining such data, parametric models have been developed. Various models have been introduced in the literature for evaluation of the CCF impact on the overall reliability of safety instrumented system including the $\beta$ factor model [39], the PDS method [22], the model of Multiple Greek Letters (MGL) [42], the α factor model [43], the Boundary model [32] and the system Cut-off model [32]. It is our understanding that a sole CCF data base initiative only exists in the nuclear industry [44–46]. Given the limitations in obtaining CCF data in the process industry in the absence of a sole database, the CCF model in this article is developed parametrically.

In this paper we use the $\beta$ factor model for assessment of CCF as recommended by IEC 61508 [11, 35]. The $\beta$ factor model is the most commonly used model due to its reasonable complexity which was initially introduced by Fleming [39]. The main assumption is that each component can fail because of:

- Events that influence only the concerned component. The corresponding failure rates for these events called independents, are denoted by $\lambda^I$.
- Events that induce simultaneous failures of the system or subsystem components. The corresponding failure rates are known as common cause and noted by $\lambda^C$.

The $\beta$ factor model comprises of a fixed proportion of the failures arising from a common cause [32]. In this model $\beta$ is usually estimated by experts using the checklist approach [46, 47].

Rahimi et al. [49] also discussed how human and organizational factors may influence CCF in SIS and outlined the challenges in assessing the $\beta$ factor. The factor $\beta$ is defined as the failure probability due to a common cause given the occurrence of a failure [30, 36] and is obtained by:

$$\beta = \frac{\lambda^C}{\lambda^T} = \frac{\lambda^C}{\lambda^I + \lambda^C} \tag{6}$$

An estimate of the value of $\beta$ is usually given by the experts to warrant a safety margin on the performance analysis results. A greater safety margin is expected with higher value, however, a reasonable selection is anticipated to compromise between safety and costs. The choice of $\beta$ directly induces the values of common cause failure ($\lambda^C$) and independent failures ($\lambda^I$) as explained by the following relations:

$$\lambda^I = (1-\beta)\lambda^T \qquad \lambda^C = \beta\lambda^T \tag{7}$$

where $\lambda^T$ is the total failure rate of a component. In accordance with the $\beta$ factor model, the total failure rate of a component is the sum of common cause and independent failures [35]:

$$\lambda^T = \lambda^I + \lambda^C = (1-\beta)\lambda^T + \beta\lambda^T \tag{8}$$

Applying the ratio determined by the $\beta$ factor model above to total failure rate in Equation (2), the detected and undetected failure modes are segregated into independent and common cause failures. The total failure rate is therefore split into eight different contributions as follows:

$$\lambda^T = \lambda^I_{DD} + \lambda^C_{DD} + \lambda^I_{DU} + \lambda^C_{DD} + \lambda^I_{SD} + \lambda^C_{DD} + \lambda^I_{SU} + \lambda^C_{DD} \tag{9}$$

As the primary objective is to determine the PFD, only the dangerous failure of the components is considered. Hence, the CCF quantification for various rates of the detected and undetected dangerous failures becomes:

$$\begin{cases} \lambda_{DD}^{I} = (1-\beta_D).\lambda_{DD} = (1-\beta_D).DC.\lambda_D \\ \lambda_{DD}^{C} = \beta_D.\lambda_{DD} = \beta_D.DC.\lambda_D \\ \lambda_{DU}^{I} = (1-\beta_U).\lambda_{DU} = (1-\beta_U).(1-DC).\lambda_D \\ \lambda_{DU}^{C} = \beta_U.\lambda_{DU} = \beta_U.(1-DC).\lambda_D \end{cases} \quad (10)$$

where $\beta_D$ and $\beta_U$ respectively represent the proportion of detected and undetected common cause failures related to the DC rate [16]. The segregation of failure rates provides an opportunity for the design engineers/analysers to study general behaviour of the system, for instance to measure the probability of system operational with only one of the components in failed states which can be used as a risk based approach for prioritisation of maintenance backlog for SRSs.

## 3.4 Inclusion of Repair Rates

### 3.4.1 1oo1 System

The system is subject to diagnostic testing as well as proof testing. The proof tests are carried out at regular time intervals of length $\tau$. For the dangerous failures detected via online diagnostic testing, the equipment downtime is equivalent to the actual repair duration. This assumes that the repair actions are instigated immediately after detection of the failure. Hence, the repair rate of dangerous detected failures, $\mu_{DD}$, is computed directly from the Mean Time To Repair (MTTR) as follows:

$$\mu_{DD} = \frac{1}{MTTR} \quad (11)$$

The equipment downtime due to dangerous undetected failures is not solely limited to the repair duration as the failure has not been revealed by an online diagnostic test and is unknown until next proof test. The undetected failures can be revealed either by

- solicitation of the equipment under control;
- proof testing assuming these tests are comprehensive and perfectly accurate (i.e. 100% detection rate) in detecting latent failures.

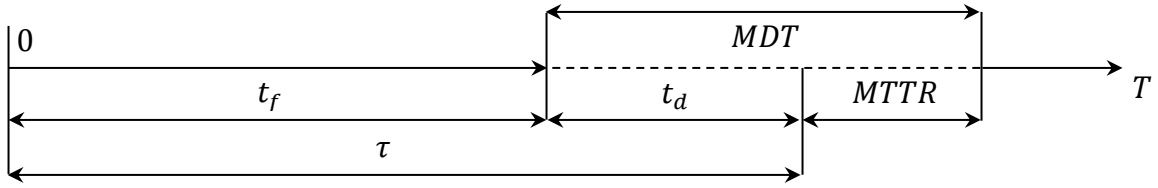


Figure 2 – Undetected Dangerous Fault Down Time

In the remaining part of this section we obtain the equipment downtime due to DU failures for a 1oo1 system. The average downtime for undetected failures may be split into two elements, known downtime and unknown downtime. The equipment downtime due to completion of the repair activity is referred to as known downtime, assuming the remedial actions are commenced immediately after detection of the failure during proof testing. The unknown downtime implies the average portion of time between occurrence of an undetected failure and its discovery during the next proof test. The time to perform a proof test is excluded from average downtime as it is often negligible. Assuming that $t_f$ is the time when the average probability of failure for a DU fault in the interval of $(0, \tau)$ occurs in a system [50], then the named equivalent Mean Down Time (MDT) for the DU fault in a channel is defined as per Figure 2 as follows:

$$MDT = \tau - t_f + MTTR \tag{12}$$

For a 1oo1 safety instrumented system the average time of failure for a DU fault is:

$$t_f = \left(\int_0^\tau t\, f(t)dt\right) / F_t(\tau) = \left(\int_0^\tau t\lambda_{DU} exp(-\lambda_{DU} t)dt\right) \Big/ \left(\int_0^\tau \lambda_{DU} exp(-\lambda_{DU} t)dt\right) \tag{13}$$

where the probability of failure in the interval of $(0, \tau)$ for the Exponential distribution is obtained from:

$$t \sim EXP(\lambda_{DU}) \rightarrow F_t(\tau) = P(t \leq \tau) = \int_0^\tau \lambda_{DU} exp(-\lambda_{DU} t)dt = 1 - exp(-\lambda_{DU}\tau) \tag{14}$$

Considering $\lambda_{DU}\tau \ll 1$ and taking into account that $exp(-\lambda_{DU}\tau) \approx 1 - \lambda_{DU}\tau$, the average time of failure for a single channel SIS is $t_f \approx {\tau}/{2}$. Where $\lambda_{DU}\tau < 0.1$, then ${\tau}/{2}$ is a sufficiently reasonable approximation to the real value of $t_f$. Therefore, Equation (12) can be written as:

$$MDT_{1oo1} = {\tau}/{2} + MTTR \tag{15}$$

As such, the DU repair rate, $\mu_{DU}$, for an undetected failure can be calculated as:

$$\mu_{DU} = \frac{1}{{\tau}/{2} + MTTR} \tag{16}$$

Of the two contributing factors to the downtime of undetected failures, the unknown part is generally dominating the overall downtime of a component. The component DD and DU failure modes and associated repairs for a 1oo1 SIS are illustrated in Figure 3.

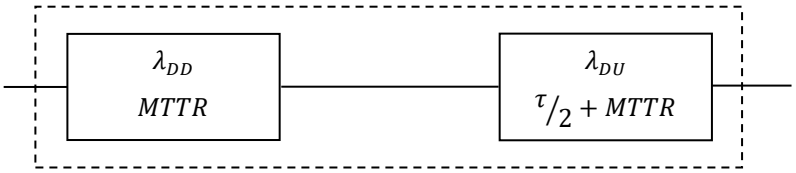


Figure 3 – 1oo1 Architecture

### 3.4.2 1oo2 System

For a 1oo2 configuration the DD repair rate is identical to the single architecture and as such can be calculated by Equation (11). This is based on the availability of the diagnostic testing and instantaneous commencement of repair action upon detection of the failure. Similar to 1oo1 simple configuration, undetected failures in a 1oo2 system can be revealed upon discharge of a demand or by conducting a proof test assuming precise testing results in detection of unrevealed failures. The MDT for a DU failure of a 1oo2 redundant architecture is derived in this section. The probability density function for undetectable fault in a redundant two component system is:

$$f(t) = \sum_{k=1}^{2} P(t \le \tau | N(t_k) = 1).P(N(t_k) = 1) \qquad (17)$$
$$= 2\lambda_{DU} exp(-\lambda_{DU} t)[1 - exp(-\lambda_{DU} t)] \qquad \text{if} \qquad t_1 = t_2$$

The average probability of failure [50] for a redundant architecture is then obtained from:

$$t_f = \left(\int_0^\tau t\, f(t)dt\right) / F_t(\tau) = \left(\int_0^\tau 2t\lambda_{DU} exp(-\lambda_{DU} t)[1 - exp(-\lambda_{DU} t)]\, dt\right) \qquad (18)$$
$$zz / \left(\int_0^\tau 2\lambda_{DU} exp(-\lambda_{DU} t)[1 - exp(-\lambda_{DU} t)]dt\right)$$

Considering for 1oo2 architecture, the probability of failure for the undetectable fault is:

$$F_t(\tau) = \int_0^\tau 2\lambda_{DU} exp(-\lambda_{DU} t)[1 - exp(-\lambda_{DU} t)]dt = [1 - exp(-\lambda_{DU}\tau)]^2 \qquad (19)$$

Since $\lambda_{DU}\tau \ll 1$ and $exp(-\lambda_{DU}\tau) \approx 1 - \lambda_{DU}\tau$, the Equation (18) is then equivalent to:

$$t_f \approx \frac{2}{3}\tau - \frac{3}{4}\lambda_{DU}\tau^2 + \frac{7}{12}\lambda_{DU}^2\tau^3 - \cdots \qquad (20)$$

As $\lambda_{DU}\tau < 0.1$, then $\frac{2}{3}\tau$ is a good approximation to the real value of $t_f$. The equivalent MDT for an undetected failure of a 1oo2 redundant architecture is thus calculated by:

$$MDT_{1oo2} = \tau - t_f + MTTR = {}^{\tau}/_{3} + MTTR \qquad (21)$$

On this basis the DU repair rate, $\mu_{DU}$, can be obtained from:

$$\mu_{DU} = \frac{1}{{}^{\tau}/_{3} + MTTR} \qquad (22)$$

In accordance with the Figure 4, the two channels and common cause component form a series system. It shall be noted that where CCF occurs, the system behaves like a single channel system and the mean down time of $MTTR$ and ${}^{\tau}/_{2} + MTTR$ are adequate representations for repair of

dangerous detected and undetected CCFs respectively. Considering the definitions of $\beta_D$ and $\beta_U$, the probability of failure for dangerous detected common cause failure [50] is $\beta_D \lambda_{DD} MTTR$ and the probability of failure for dangerous undetected common cause failure is acquired from $\beta_U \lambda_{DU} ({}^{\tau}/_{2} + MTTR)$.

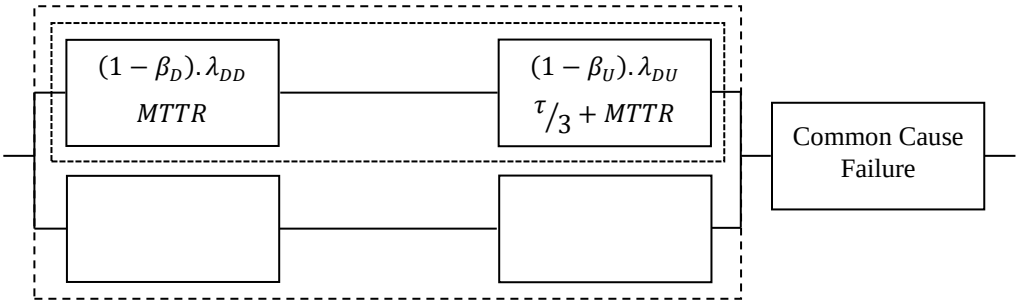


Figure 4 – 1oo2 Architecture

The repair rates for dangerous and common cause failures are embedded within the reliability model proposed in this paper in parametric form. The case study in section 5 however will take account of the repair rate values accordingly.

## 3.5 Demand Parameters & System Renewal

The process demands (PD) are assumed to occur according to a Homogeneous Poisson Process (HPP) [51] with rate $\lambda_{DE}$, hence the time between two consecutive demands is exponentially distributed with parameter $\lambda_{DE}$.

$$N_{PD} \sim POI(\lambda_{DE}) \rightarrow T_{PD} \sim EXP(\lambda_{DE}) \tag{23}$$

Assuming that the system is "as good as new" after a successful response to a process demand, the duration of each process demand (DD) is presumed to follow exponential distribution with the rate $\mu_{DE}$. Hence, the mean demand duration is computed from:

$$T_{DD} \sim EXP(\mu_{DE}) \rightarrow E(t) = {}^{1}/_{\mu_{DE}} \tag{24}$$

Moreover, when a hazardous event occurs, we assume that the system is restored / renewed to the normal available state. The system renewal (SR) rate is also considered to be exponentially distributed with rate $\mu_T$.

$$T_{SR} \sim EXP(\mu_T) \rightarrow E(t) = {}^{1}/_{\mu_T} \quad (25)$$

## 3.6 Model Assumptions

The following underlying assumptions are made as a basis for developing a new reliability model in this paper:

- The time to failures are exponentially distributed (all failure rates are constant in time).
- All safe and dangerous failures occur independently (separately) and their magnitudes are constant over time.
- The redundant elements considered are identical and have the same constant failure rates.
- The $\beta$ factor model is used to consider the CCFs; however, the reliability model can be easily extended to accommodate different CCF models.
- The time between demands is exponentially distributed (process demand rate is constant).
- The process demand duration and restoration time from hazardous state are exponentially distributed.
- The rate of independent (ID) failures is segregated from the total failure rate, such that $(1-\beta_U)\lambda_{DU}$ is used instead of $\lambda_{DU}$ for independent DU failures. Subsequently CCF rates, $\beta_U\lambda_{DU}$, leading to subsystem failure are clearly identified for redundant subsystems.
- Proof tests are comprehensive (100% accurate) and carried out periodically in line with the specified test intervals of the system.
- A single maintenance team is available on site.
- The system can be considered “as good as new” upon completion of a repair or a proof test.

## 3.7 Markov Chain based Reliability Model

Reliability modelling using Markov chains is one of the techniques quoted in IEC 61511 [1]. Markov chains are a holistic approach frequently used in dependability analysis for modelling a repairable system where components fail at constant failure rate and are repaired at constant

restoration rates [16]. In this paper, the transition probabilities of Markov chain are considered independent of time and following the homogeneous process therefore, the failure / repair rates are considered constants. This assumption is consistent when working in the useful life period (maturity phase) of components. It is also possible to take into account some dependencies in Markov chains in order to perform a dynamic analysis of the system [19]. A Markov chain is a model that transits from state $i$ to state $j$ with a probability $p_{ij}$ which depends only on the states $i$ and $j$. The transition matrix $\boldsymbol{P} = [p_{ij}]$ be $(r \times r)$ constructed from all transition probabilities $p_{ij}$:

$$\boldsymbol{P} = [p_{ij}] = \begin{bmatrix} p_{11} & p_{12} & \cdots & \cdots & p_{1r} \\ p_{21} & p_{22} & \cdots & \cdots & p_{2r} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{r1} & p_{r2} & \cdots & \cdots & p_{rr} \end{bmatrix} \tag{26}$$

Assuming $P(t) = [P_1(t), \dots, P_r(t)]$, where $P_j(t)$ represents the probability of finding the system in state $j$ at time $t$. The transition law of a Markov chain is defined by the following equation:

$$[P_1(t), \dots, P_r(t)] = [P_1(t-1), \dots, P_r(t-1)]. \begin{bmatrix} p_{11} & p_{12} & \cdots & \cdots & p_{1r} \\ p_{21} & p_{22} & \cdots & \cdots & p_{2r} \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ p_{r1} & p_{r2} & \cdots & \cdots & p_{rr} \end{bmatrix} \tag{27}$$

Equation (27) can be written in a compact form as follows:

$$P(t+1) = P(t).\boldsymbol{P} \tag{28}$$

Considering that $\boldsymbol{P}$ is a probability matrix, the sum of each row of $\boldsymbol{P}$ is one and all the coefficients $p_{ij}$ are equal to or greater than zero. The probability of each state $j$ at each time $t$ is given by:

$$P_j(t) = \sum_i P_i(t-1).p_{ij} \tag{29}$$

If $P(0) = [P_1(0), \dots, P_r(0)]$, where $P_j(0)$ is the probability of being initially in state $j$. The Chapman-Kolmogorov formula [11] is obtained from Equation (28) as follow:

$$P(t) = P(0).\boldsymbol{P}^t \tag{30}$$

A property of regular Markov chains is that powers of $\boldsymbol{P}$ converge to a vector of probabilities $\boldsymbol{\Pi}$. The vector $\boldsymbol{\Pi} = [\pi_1, \dots, \pi_r]$ represents the steady state probabilities and can be determined by solving the following linear system [11]:

$$\boldsymbol{\Pi}.\boldsymbol{P} = \boldsymbol{\Pi} \tag{31}$$

The steady state probability for state $i$, $\pi_i$, is the long-run probability that the system is in state $i$. It also signifies the mean proportion of time the system is in state $i$ [3] and the fact that the sum of the steady state probabilities is always equal to 1.

$$\sum_{i=1}^{r} \pi_i = 1 \tag{32}$$

The unavailability of the safety system is computed by summing the probabilities of being in states $j$ at each time $t$, according to Equation (33) where $j$ corresponds to the states that the safety system is not able to respond on demand:

$$PFD = \sum_{j} \pi_j \tag{33}$$

In a Markov model, the frequency of entering a hazardous state can be acquired directly from the transition diagram. The system transits to the hazardous state when a demand is inflicted on it whilst the SIS is failed dangerously either detected or undetected. The hazardous event frequency (HEF) is equal to the visit frequency to state 0, from any other possible states [11]:

$$HEF = \sum_{i=1}^{r} q_{i0}\, \pi_i \qquad \text{where} \qquad q_{ij} = \frac{d}{dt} p_{ij}(t) = \lim_{t \to 0} \frac{p_{ij}(t)}{t} \tag{34}$$

In this article, we aim to investigate the reliability performance of safety related systems where redundancy in components is embedded within the architectural design of the system. This considers the demand rate and duration of demand for safety related systems operating in various demand modes. A generic framework for reliability assessment of redundant safety instrumented systems subject to demand using Markov chains is illustrated in Figure 5. This framework

outlines steps required for completion of the reliability assessment including SIS definition, demand analysis, component failure and repair data, test strategies and lastly the implementation of the safety instrumented systems. Additionally, the reliability assessment framework can be used in conjunction with the safety lifecycle plan as outlined by the international standard IEC 61508 and can be applied to all E/E/PES safety related systems.

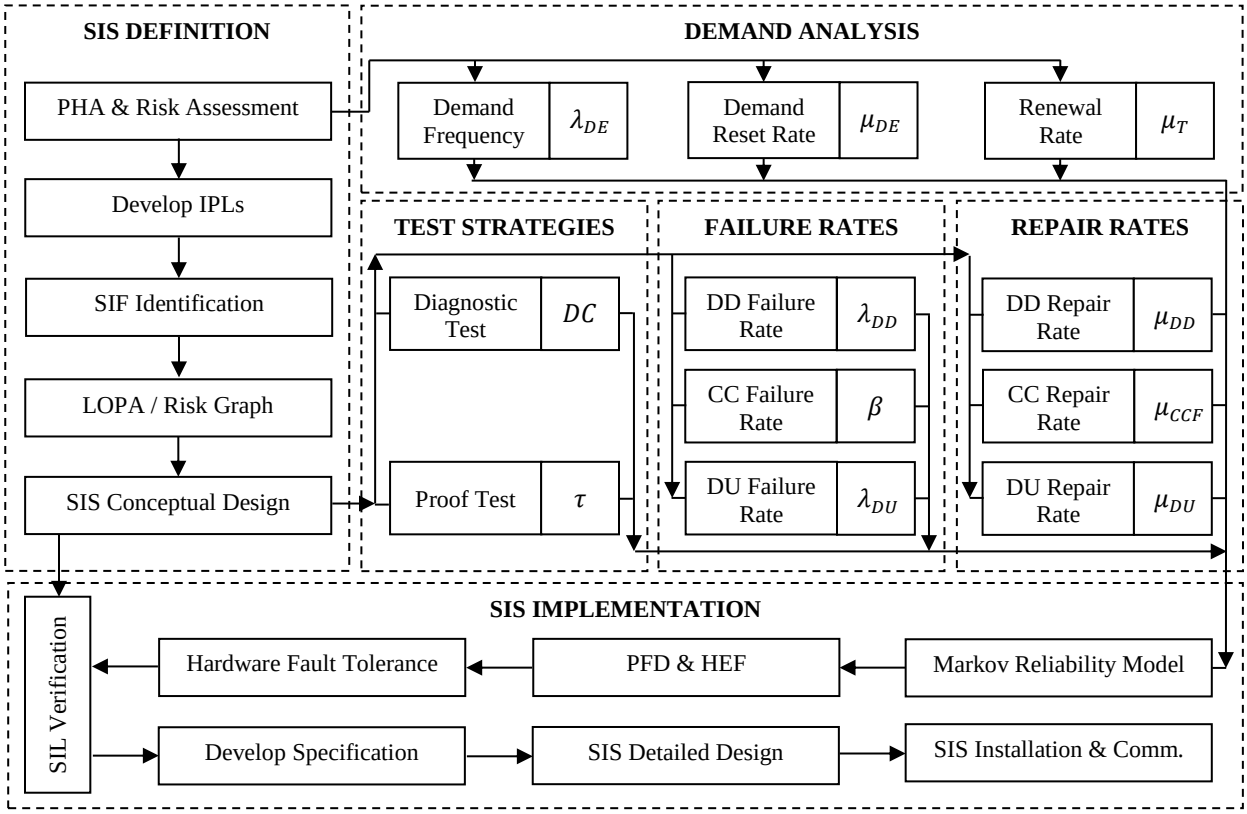


Figure 5 – Framework for Reliability Assessment for Redundant Safety Instrumented Systems Subject to Demand

Various studies [3, 16] have considered PFD as steady state unavailability using Markov methodology whereas others as average value of unavailability in line with IEC 61508 [1]. Nevertheless, the authors acknowledge that the steady state unavailability computed in this paper is not the same as, nor equivalent to the $PFD_{avg}$ required for SIL verification in IEC 61508 and IEC 61511. However, when using the models presented, the calculated steady state unavailability is greater than the $PFD_{avg}$ defined in IEC 61508/61511 that would have been computed from the same models. The steady state unavailability is therefore conservative and considered an acceptable substitute for $PFD_{avg}$.

# 4.0 Analysis of Safety Related Systems

## 4.1 Markov Model for 1oo1 SRS

A Markov model for a simple 1oo1 safety instrumented system was originally developed by Rausand & Høyland [11]. The application of this model is reviewed in this paper for a simple safety related system, a Pressure Relief Valve (PRV). It should be noted that PRVs are normally considered as mechanical devices and are not categorised as a safety instrumented system since the two primary elements of SIS including sensor / transmitter and logic solver elements of the system do not exist. However, considering PRV as the final element of a SIS, the Markov model developed for SIS can be simplified to represent the failures modes of mechanical safety devices such as a PRV. In other words, the 1oo1 PRV is an exceptional case of generic SIS model with process demand incorporated. The primary dangerous failure mode for a PRV is "fail to open" on demand. In accordance with PDS Data Handbook [52] the DD failure rate for a PRV is 0 and hence only DU failure rate is incorporated within the model. The dynamic of SRS consists of the combined characteristics of the system state and demand levied on the safety system. A safety related system is defined as "available" when it can respond to a demand upon manifestation. This means that the safety related system is not failed due to DU failure and has not been spuriously activated. The SRS is considered in "functioning" state when it is reacting to a process demand. The possible states of the system are outlined in Table 2.

Table 2 – States of 1oo1 SRS

| System State | Property | Demand State |
|---|---|---|
| 0 | Hazardous | On Demand |
| 1 | Available | No Demand |
| 2 | Functional | On Demand |
| 3 | DU Failure | No Demand |
| 4 | Safe Failure | No Demand |

State 1 denotes the initial and normal operating state in the Markov transition diagram, where the safety system is available but there is no demand for activation of the safety function. The safe state (e.g. spurious activation) is represented by state 4 indicating that the EUC is safe regardless of whether there is a demand or not and hence no hazardous event can occur at this stage. Safe

failure modes of PRV comprised of “spurious operation”, “fail to close” and “leakage in closed position”. The transitions between states 1 and 4 are due to safe failure and restoration. The safe state 4 is incorporated for modelling purpose however it is noted that the system PFD is characterised by dangerous failures only. State 2 represents the functioning state where the SRS is responding to a process demand. Upon removal of the process demand the safety system goes back to state 1. The system transits to state 3 from state 1 due to DU failure while there is no process demand levied on the SRS. Repair of the DU failure will lead to system transition to the available state by the corresponding repair rate $\mu_{DU}$. State 0 (hazardous state) represents a state where the SRS sustains a failure and there is a demand for activation of the SRS. The system enters hazardous state 0 from state 2 when the safety system is impaired due to a DU failure as it is responding to a process demand. Alternatively, the hazardous state 0 is reached from state 3 if a process demand is imposed on the SRS whilst it is in failed state. The Markov transition diagram is illustrated in Figure 6 where arrows represent system transition from one state to another and the nodes correspond to the systems states.

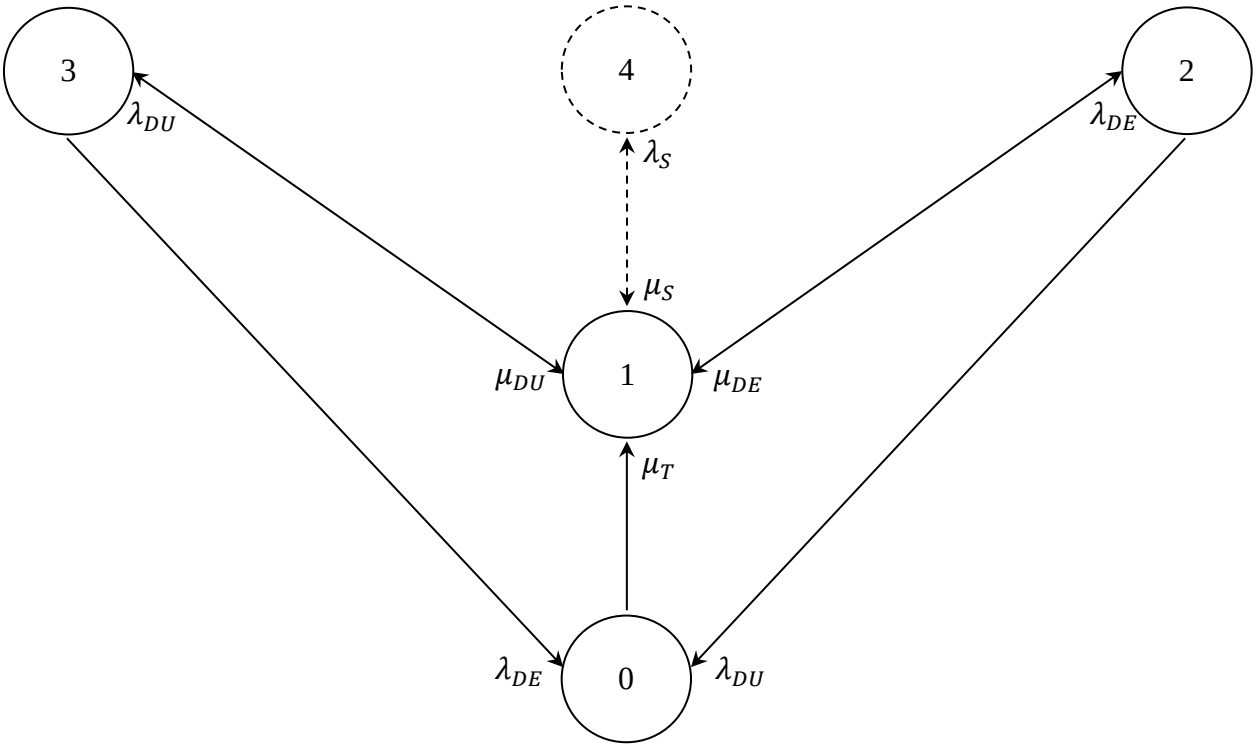


Figure 6 – Markov Transition Diagram for a 1oo1 SRS

A restoration action is initiated, when system enters the hazardous state (state 0) and the system is started up again in an “as good as new condition” in state 1. The mean time required to restore

the system from state 0 to state 1 is $1/\mu_T$ as per Equation (25). The relevance of this assumption may differ and for some applications start up after a hazardous event may not be feasible. In a worst credible event scenario, the entire system and/or plant may be demolished due to the consequence of the hazardous event. However, the restoration rate from hazardous state is an essential element of the Markov model since it eliminates absorbing state (state 0) and enables calculation of the steady state probabilities. To avoid this problem, we may instead consider the hazardous state(s) as absorbing state(s), and calculate the mean time from start-up in perfect state until a hazardous state takes place [11]. The steady state equations from the state transition diagram in Figure 6 for 1oo1 SRS can be obtained from:

$$\begin{aligned}
&\mu_T P_0 = (\lambda_{DU} P_2 + \lambda_{DE} P_3) \\
&(\mu_{DE} + \lambda_{DU}) P_2 = \lambda_{DE} P_1 \\
&(\mu_{DU} + \lambda_{DE}) P_3 = \lambda_{DU} P_1 \\
&\lambda_S P_1 = \mu_S P_4
\end{aligned} \tag{35}$$

The sum of steady state probabilities is unity considering that the system will be in one of the states in infinity, $\sum_i P_i = 1, i = 0, \ldots, 4$.

## 4.2 Markov Model for 1oo2 SRS

A classic formation of safety related systems is two identical channels connected in parallel known as 1oo2 where the protective function can be implemented if one of the two components is operational as a minimum. Therefore, only a dangerous failure in both channels results in failure of the safety function on demand. Despite enhancing the system availability, provision of redundancy may however present CCF which takes place when two or more components fail concurrently due to a common stressor. Liu et al. [19] developed a reliability model for 1oo2 safety system on the foundation of simple structure discounting CCF. In this section, we intend to develop a new Markov model for a 1oo2 redundant safety related system by inclusion of CCF in conjunction with incorporating demand for the first time. The generic underlying assumptions itemised for simple system are all valid for 1oo2 SRS. The possible states of the system are outlined in Table 3 and the Markov transition diagram is illustrated in Figure 7:

Table 3 – States of a 1oo2 SRS

| State | Property | Demand State |
|---|---|---|
| 0 | Hazardous | On Demand |
| 1 | 2 DU | No Demand |
| 2 | 1 Functional, 1 DU | On Demand |
| 3 | 1 Functional, 1 DU | No Demand |
| 4 | 2 Functional | On Demand |
| 5 | CCF | No Demand |
| 6 | Available | No Demand |
| 7 | Safe | N/A |

Similar to the simple configuration, the 1oo2 safety related system consists of the combined effect of the SRS states and process demand levied on the safety system. The process demand and its reset rates as well as renewal rate for the 1oo1 system can be adopted for a 1oo2 SRS, on the basis that the redundant configuration can be employed as a replacement in kind to the simple architecture and in the same industrial application to enhance reliability. The system transitions due to dangerous undetected failure rate, $\lambda_{DU}$, and associated repair, $\mu_{DU}$, are intact. However, similar to 1oo1 simple system, DD failures, $\lambda_{DD}$, and associated DD repair rate, $\mu_{DD}$, are excluded from the reliability model since the DD failure rates, $\lambda_{DD}$, for PRV are annulled. Change to the system dynamics due to safe failure rate, $\lambda_S$, either detected or undetected and its subsequent repair rate, $\mu_S$, are entailed within the proposed model, consistent with the simple structure. The system transition rates in the 1oo2 redundant safety system is $\lambda_{DU}^I$ for independent failures and $\lambda_{DU}^C$ for undetected CCFs where $\beta_U$ represents the undetected CCF factor.

Starting with system in "available" status and no process demand (i.e. state 6), the safety system fails safely and transits to state 7 with failure rate $2\lambda_S$ and reinstated to state 6 with safe repair rate $\mu_S$. The system unavailability solely due to safe failures is not foreseen in this reliability model since failure of both components (sequential or concurrent) is not embedded within the Markov chain. Similar to the simple configuration, the safe state 7 is illustrated for modelling purpose and has no impact on system's reliability performance. The safety system is responding to a process demand in state 4 with both components functional. Upon fulfilment of the process demand the system transits back to the original state 6. The transition rate from state 6 to 3 is the

minimum of two independent dangerous undetected failures, $2(1-\beta_U)\lambda_{DU}$. This excludes the dangerous undetected CCFs since any of the components can fail independently. An identical transition occurs between state 4 and 2 whilst the system is responding to a demand. The system will transit to the "available" states 6 (from state 3) or "fully functional" state 4 (from state 2) when the failed component is repaired with $\mu_{DU}$ repair rate during the next proof test interval.

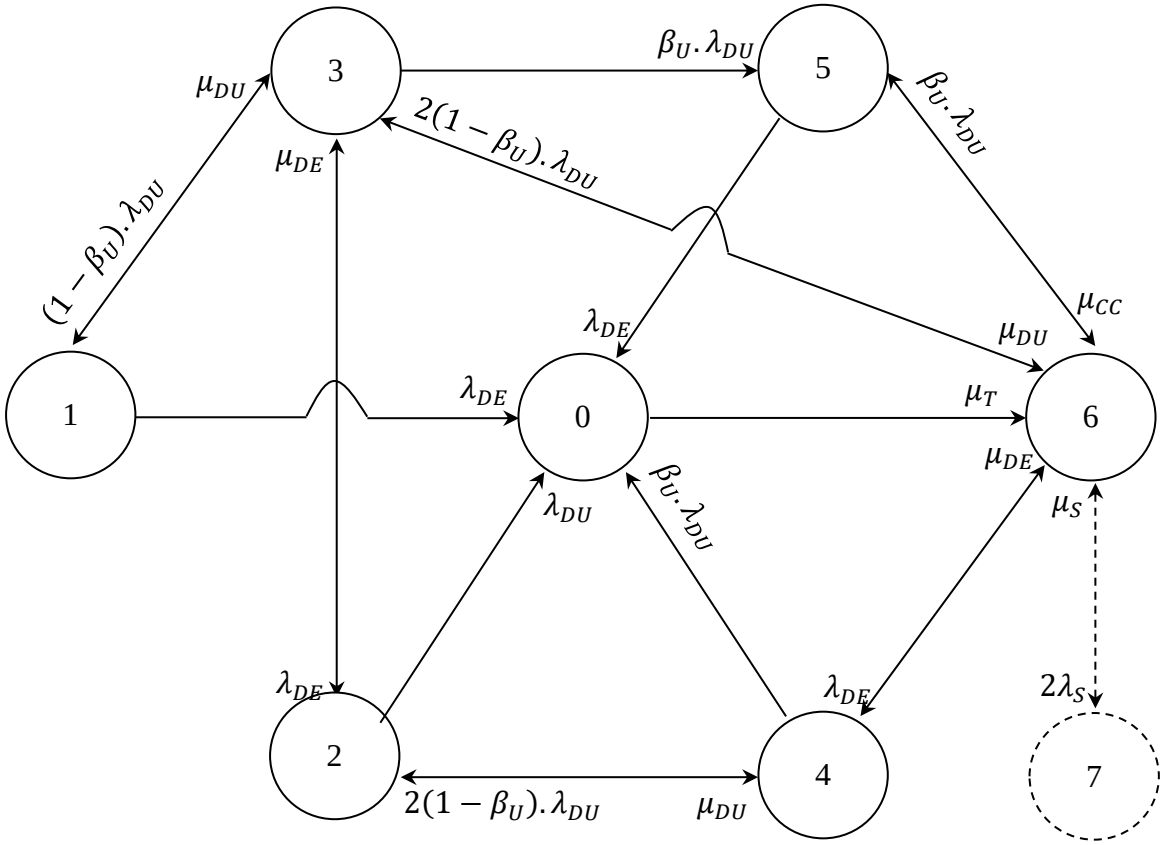


Figure 7 – Markov Transition Diagram for a 1oo2 SRS

In state 2, the safety related system is responding to a process demand with only one component functioning whereas in state 3 no demand is levied on the system. The safety system alternates between states 2 and 3 depending on manifestation of a process demand or removal of the demand when it terminates. Single DU or spurious activation does not impair system ability to respond to a process demand and hence has no impact on its availability is envisaged. In this case safety system is still defined as in "functioning" state. The system conveys to state 1 from state 3 upon occurrence of a DU failure, $(1-\beta_U)\lambda_{DU}$, resulting in failure of the remaining functioning component. This means that in state 1 the safety system endures two consecutive DU failures and

hence no longer functional. Subsequently, the system can be reinstated to the original "available" state post completion of two repairs in succession.

The CCF can occur on four separate occasions, one of which is when an individual component is in failed state whilst the other component is still functional. Example of this scenario is excessive vibration of instrument tubing pipework leading to the failure of the remaining level temperature transmitter whilst the other field transmitter already failed due to a separate cause. In this regard a shift from state 3 to state 5 is practical with $\beta_U \lambda_{DU}$ common cause failure rate when there is no demand imposed on the system. On the other hand, a CCF transpires during an on demand transition from state 2 to state 0 when one of the components is in failed status and the remaining component is functional and responding to a process demand. Additionally, a CCF may take place when system is in "available" state and there is no demand resulting in system transition from state 6 to state 5 with $\beta_U \lambda_{DU}$ failure rate. The CCF can also arise when system is responding to a process demand in state 4 leading to a system transition to the hazardous state 0 with the same failure rate. It is assumed that repair of CCFs are carried out in a single stage repair and as such sequential repair of individual components is not deemed necessary. As such, the system transits from state 5 to state 6 in a singular transition and no consecutive repair for CCF is considered in this model.

The hazardous state (state 0) represents a situation when the safety system sustains a failure and there is a demand for activation of the safety function. The hazardous state 0 is reached when both components are failed either due to two sequential undetected failures (6-3-1), a combination of DU and CCF (6-3-5), or a standalone CCF (6-5); and a demand arises with $\lambda_{DE}$ rate. Alternatively, emergence of a CCF in state 4 when system is responding to a process demand with two components fully functional (6-4) leads to a hazardous event. The system also visits hazardous state when it fails dangerously whilst responding to a process demand. In this circumstance, the system visits hazardous state from state 2 where the system is responding to a process demand with the only remaining functional component (6-4-2) and it fails dangerously, either due to single DU or CCF, resulting in impairment of the protection layer and exposure to a hazardous event. A restoration action is instigated when the system enters the hazardous state 0. Upon completion of the restoration with mean time $1/\mu_T$, the system is started up again in an "as good as new condition" in state 6. This is only achievable where the hazardous event is either

repeatable or renewable in accordance with the classification identified by Youshiamura [53]. No transition from state 0 to states 1, 2, 4 and 5 is considered in this model post occurrence of a hazardous event.

It is crucial to highlight that the aforementioned scenarios involve common cause and dangerous undetected failures only and do not encompass DD failures. Moreover, it is assumed that only one component can be repaired at a time since only one maintenance team is available onsite. The primary property of any Markov process also known as Markov property is that the future status of the system depends on the current status of the system only and is independent of its past circumstances. This property is embedded within the Markov chain developed for the 1oo2 SRS as a memoryless system. Furthermore, the system fulfils the secondary feature of Markov process recognised as stationary property in which the transition probabilities from one state to another state remain constant with time. As such, the steady state probabilities ($\pi_i, i = 0, \dots, 7$) can be derived from the transition diagram. The steady state equations corresponding to the Markov transition diagram in Figure 7 for 1oo2 SRS are as follows:

$$
\begin{aligned}
&(\lambda_{DE} + \mu_{DU} + \lambda_{DU})P_3 = 2(1-\beta_U)\lambda_{DU}P_6 + \mu_{DE}P_2 + \mu_{DU}P_1 \\
&(\mu_{DU} + \lambda_{DU} + \mu_{DE})P_2 = 2(1-\beta_U)\lambda_{DU}P_4 + \lambda_{DE}P_3 \\
&(\mu_{DE} + (2-\beta_U)\lambda_{DU})P_4 = \lambda_{DE}P_6 + \mu_{DU}P_2 \\
&\mu_T P_0 = \lambda_{DE}(P_5 + P_1) + \lambda_{DU}(\beta_U P_4 + P_2) \\
&(\mu_{CC} + \lambda_{DE})P_5 = \beta_U \lambda_{DU}(P_6 + P_3) \\
&(\mu_{DU} + \lambda_{DE})P_1 = (1-\beta_U)\lambda_{DU}P_3 \\
&\mu_S P_7 = 2\lambda_S P_6
\end{aligned}
\tag{36}
$$

Similar to the 1oo1 simple system the summation of steady state probabilities is unity taking into account that the system alternates between all possible states, $\sum_i P_i = 1$, $i = 0, \dots, 7$. The effect of Proof Test Coverage (PTC) was overlooked in various publications including studies based on Markovian methodology [3, 19, 49] and those that employed non-Markovian techniques [23] on the basis of comprehensiveness (100% detection rate) of proof tests. This is also apparent in the IEC 61508 approach since the formulae do not entail the effects of non-comprehensive proof testing [36]. Likewise, the evaluation of proof test coverage was not explored further in this paper on the basis that proof tests are comprehensive. However, in accordance with the latest

edition of IEC 61511 (2016), if the proof tests are not 100% accurate, then the PTC ratio shall be considered. This enables the analysers/designers to account for the DU failures which can never be detected by proof tests, as well as to account for DU failures which can be found by complete execution of proof tests but which will be missed if proof tests are not completely executed. Incorporation of PTC within the reliability model may potentially lead to substantial alteration in the structure of the Markov chain and therefore subject to a thorough analysis of the model's behaviour prior to incorporation of PTC as an additional variable. The proposed reliability model in this paper however provides a foundation to include the PTC in the next phase of its development.

## 4.3 Markov Reliability Performance Indicators

When a safety related system is utilised to reduce risk, IEC 61508 [4] stipulates requirements to demonstrate that the reliability performance of safety system is adequate to satisfy the specified risk acceptance criteria. The acceptance criteria are often stated in terms of a maximum tolerable HEF, from which a SIL requirement, and eventually, a PFD requirement may be deduced [1, 4]. It is noted that PFD should in principle, cover both the instantaneous activation of the SRS and the successful performance of the system during the demand period. In practice, most calculation approaches fail to account for the possibility of having a failure during the demand period. As such, the PFD is well suited as input parameter to many methods for risk analysis including but not limited to fault tree analysis, event tree analysis, and LOPA [2]. In this regard, PFD and HEF are used in this paper to measure and compare the performance of the proposed reliability model of 1oo2 redundant configuration versus established simple structure.

Table 4 – Markov Performance Indicators for 1oo1 & 1oo2 Safety Related Systems

| Model | PFD | HEF |
|---|---|---|
| 1oo1 SRS | $P_3$ | $\lambda_{DE}P_3 + \lambda_{DU}P_2$ |
| 1oo2 SRS | $P_1 + P_5$ | $\lambda_{DE}(P_5 + P_1) + \lambda_{DU}(\beta_U P_4 + P_2)$ |

The 1oo1 SRS system will not be able to respond to a process demand when it is in state 3 whereas the 1oo2 SRS will not be able to respond to a process demand when it is in states 1 or 5. Furthermore, the frequency (per hour) of entering into the hazardous state is equivalent to the visit frequency to state 0, from any other state. The PFD and HEF for the 1oo1 safety system are

given in Table 4. For a low demand SRS, HEF is the product of the demand rate, $\lambda_{DE}$, for the SRS and the conditional probability that the SRS fails to function, PFD, given a demand, such that $HEF \approx PFD.\lambda_{DE}$. This is in line with the Markov models developed in this paper for 1oo1 and 1oo2 configurations.

## 4.4 Markov Model vs IEC 61508 Approach

A comparison between the Markov models proposed in this paper and IEC 61508 approach for single structure and redundant configurations of safety related systems are provided in this section. In addition to the assumptions listed in section 3.6 the following principles are adopted in line with IEC 61508 general philosophies for determination of SRS reliability performance:

- dangerous detected failure rate for the PRVs is annulled and hence discarded;
- process demand is not incorporated within the IEC 61508 reliability calculation;
- safe failures are excluded by IEC 61508 approach for evaluating reliability of SRSs.

### 4.4.1 IEC 61508 Approach for 1oo1 SRS

The reliability performance of 1oo1 SRS for pressure relief valve can be calculated directly in accordance with IEC 61508 [4]. Noting the underlying assumptions, the pictorial representation of IEC 61508 approach for a 1oo1 SRS is shown in Figure 8 with only DU failure dictating the system unavailability. It is to be noted that Figure 8 is the authors' Markov model interpretation of the IEC 61508 approach for DU failures and repairs in a 1oo1 safety architecture, it does not appear in IEC 61508.

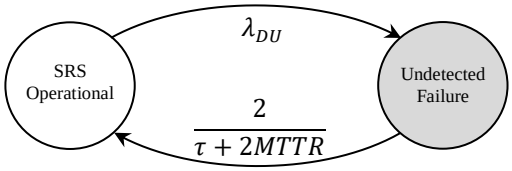


Figure 8 – IEC 61508 Approach for DU Failure & Repair Rates of 1oo1 SRS

In this case the channel MDT is obtained directly from Equation (15). The average probability of failure on demand for a 1oo1 architecture provided by the IEC 61508 standard can also be simplified as function of component failure rate and mean down time as follows:

$$PFD_{1oo1} = \lambda_{DU}({}^{\tau}/_{2} + MTTR) \quad (37)$$

Comparison between the 1oo1 Markov model (Figure 6) and IEC 61508 approach (Figure 8) illustrates the over simplistic approach taken by the latter in quantifying reliability performance of the safety related system. In this case due to elimination of safe failures and exclusion of demand parameter the Markov chain is rationalised to a single stage transition between the operational status of the SRS and unavailability of the systems due to DU failure mode. In this case if $\lambda_D MTTR \ll 0.1$, one can justify that the conventional ${}^{1}/_{2}\,\lambda_{DU}\tau$ is a good approximation to the value of PFD for the 1oo1 safety related system.

### 4.4.2 IEC 61508 Approach for 1oo2 SRS

Similar to the simple system, the reliability performance of 1oo2 SRS can be calculated directly in accordance with the international standards. The IEC 61508 [4] approach for the 1oo2 SRS redundant configuration is demonstrated in Figure 9. It is observed that the number of transition nodes is half of the Markov model due to exclusion of process demand. Despite complexity of Markov models for reliability analysis of SRSs subject to process demand, the thoroughness, flexibility and accuracy of such a reliability model outstrips its disadvantages of use. This Figure 9 is the authors' Markov model interpretation of the IEC 61508 approach for DU failures and repairs in a 1oo2 safety architecture, it does not appear in IEC 61508.

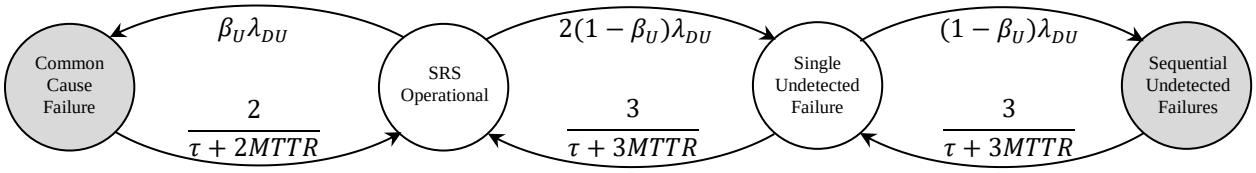


Figure 9 – IEC 61508 Approach for CCF, DU Failure & Repair Rates of 1oo2 SRS

The average probability of failure on demand can be calculated as probability of system being in states "Common Cause Failure" OR "Sequential Undetected Failures". The average probability of failure on demand for the 1oo2 architecture provided by the IEC 61508 [4] standard can then be simplified as follows:

$$PFD_{1oo2} = 2\left[\lambda_{DU}(1-\beta_U)\left[{}^{\tau}/_{3} + MTTR\right]\right]^2 + \beta_U\lambda_{DU}({}^{\tau}/_{2} + MTTR) \quad (38)$$

Although the reliability calculation of 1oo2 SRS proposed by the standard appears to be simpler and requires minimum computational effort, the dynamic behaviour of the system due to imposition of process demand is ignored.

### 4.4.3 IEC 61508 Reliability Performance Indicators

The PFD and HEF performance indicators for the 1oo1 and 1oo2 SRS based on IEC 61508 approach are listed in Table 5. The HEF is derived from $HEF \approx PFD.\lambda_{DE}$ using the conditional probability of SRS failure given imposition of a demand.

Table 5 – IEC 61508 Performance Indicators of 1oo1 & 1oo2 Safety Related Systems

| Model | PFD | HEF |
|---|---|---|
| 1oo1 SRS | $PFD_{1oo1}$ | $\lambda_{DE}PFD_{1oo1}$ |
| 1oo2 SRS | $PFD_{1oo2}$ | $\lambda_{DE}PFD_{1oo2}$ |

The simple SRS system will not be able to respond to a process demand when it is in DU state. The redundant SRS on the other hand will not be able to respond to a process demand when it is in states “Common Cause Failure” OR “Sequential Undetected Failures”. When using these indicators the operability of the SRS in low demand mode of operation shall be ensured to satisfy the eligibility criteria although the value of the process demand is an irrelevant factor here.

# 5.0 Application: Study of a Tank Pressure Protection System

To validate the proposed model, a flammable Liquid Storage Tank (LST) [54,55] has been undertaken in this paper as a case study. The Piping & Instrumentation Diagram (P&ID) of the flammable liquid storage tank is illustrated in Figure 10. The equipment and field instrumentation notations used in the P&ID are provided in Table 6 in a tabular format.

Table 6 – LST Equipment & Instrumentation Notation

| Equipment & Valves | | Field Instrumentation | |
|---|---|---|---|
| FCV | Flow Control Valve | FIC | Flow Indicator Controller |
| LST | Liquid Storage Tank | FT | Flow Transmitter |
| PCV | Pressure Control Valve | LAH | High Level Alarm |
| PRV | Pressure Relief Valve | PAH | High Pressure Alarm |
| PZ | Centrifugal Pump | PI | Pressure Indicator |
| V | Isolation Valve | PIC | Pressure Indicator Controller |

The LST is designed to store flammable liquid hydrocarbon supplied by trucks under slight positive nitrogen pressure. Nitrogen is used as a blanket gas to prevent ingress of oxygen and eliminate formation of a stoichiometric mixture within the ullage space of the tank. The controller PIC maintains the positive pressure within the tank via Pressure Control Valves ($PCV_1$ and $PCV_2$). Tank liquid level and internal pressure is monitored via field instrumentation, LAH and PAH. The tank is fitted with a redundant pressure relief system ($PRV_1$ and $PRV_2$) to release the excess liquid in an emergency. A centrifugal pump (PZ) is installed downstream of the tank to supply the liquid to the process plant. The PI monitors the pump discharge pressure and the discharge flow is controlled via a Basic Process Control System (BPCS) consisting of a Flow Transmitter (FT), a Flow Controller (FIC) and a dedicated Flow Control Valve (FCV).

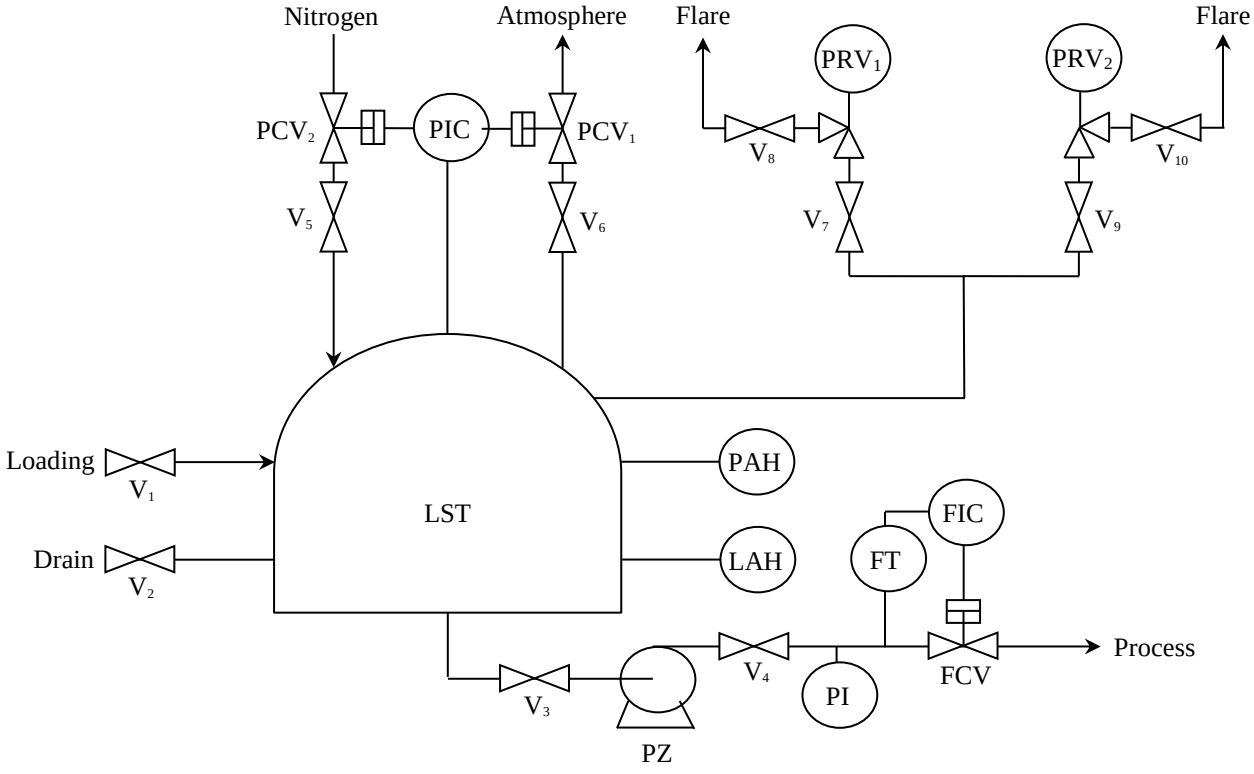


Figure 10 – Flammable Liquid Storage Tank P&ID

Various manual valves ($V_1$ - $V_{10}$) are installed to allow isolation and maintenance of equipment. The tank can also be drained for maintenance and inspection purposes. The system is operational in continuous mode to feed the downstream facilities. The LST and associated equipment are located on an onshore plant and segregated from the main process units by distance.

## 5.1 Layers of Protection

Various layers of protections are embedded within the design of the LST to prevent the rise of the liquid level and mitigate its consequences. These protection layers consisting of instrumentation and mechanical devices as demonstrated in the P&ID are as follows:

- Instrument IPLs: rise of the liquid level will result in initiation of the LAH which requires operator action to shut down the process system and cease the incoming flow. The liquid rise within the tank will also result in elevation of LST internal pressure. The PAH will then alert the operator of any deviation in operating limits to allow remedial action to be undertaken. There is no automated instrument shutdown (i.e. SIS) included within the design.
- Mechanical IPLs: where the critical alarms (CAs) fail to initiate OR the operator fails to respond to the alarms, the tank pressure relief system will be activated. The PRVs will direct excess liquid to the flare system for disposal. The overpressure protection system designed for the tank consists of two redundant PRVs in parallel. Each PRV is fully sized and provide 100% relief capacity for full release of liquid. As such, availability of only one PRV at any time would suffice. The set pressures of the PRVs are identical and calculated at above tank operating pressure but below its design envelope to maintain the integrity of the tank. The reliability performance of a redundant PRV system versus sole PRV configuration will be the focus of this case study to assess the application of the proposed model.

It shall be noted that the use of parallel connection of identical channels is not always the correct way to implement a 1oo2 safety architecture. There is a distinction between so called “reliability architectures” in which success depends on the connectivity from input to output, and “safety architectures” where success relies on the ability to disrupt continuity.

## 5.2 Process Demand

Process demand on the PRVs will be initiated by uncontrolled rise of the liquid level resulting in pressure spike within the tank. The underlying causes of liquid rise within the LST are comprised of the following:

- uncontrolled loading operation resulting in rise of the liquid level within the tank; AND
- failure of the tank downstream equipment such as
    - pump failure; OR

- closure of the isolation valves ($V_3$ and/or $V_4$); OR
- malfunction of the flow control ancillary equipment (FT, FIC and/or FCV).

The aforementioned underlying causes in conjunction with the failure of the IPLs results in generating demand on PRVs. Therefore, to quantify the frequency of process demand it is necessary to evaluate each of these causes and assess the likelihood of combined failures in the logical sequence as identified by the process hazard analysis.

## 5.3 Hazardous Event & Consequence Assessment

The uncontrolled rise of the flammable liquid level within the LST, will result in over pressurisation of the tank. This hazard will be prevented by the PRVs by releasing the excess flammable liquid into the flare system. It is assumed that the flare system is suitably designed to handle excess fluids and an automatic action will be initiated by a robust level control system in the flare knock out drum to restore the process to the original status within its operating limits. No damage to the equipment in this scenario is envisaged since the release to the flare system reduces the tank pressure. As such, the extent of the hazardous event in this case is limited to environmental damage only and is considered as a repeatable hazard [53].

Failure of the pressure relief system to open on demand as the last protection layer whilst the liquid level is continuously rising within the tank, will result in over pressurisation of the tank and ultimately impairment of the tank integrity and pipework / tank rupture leading to loss of containment. The tank is equipped with a dedicated bund which is suitably sized for a full-size rupture and hence, the flammable liquid will be removed when released to reduce personnel exposure to hazardous / toxic material. It is assumed that upon loss of containment, the plant Fire & Gas (F&G) system will initiate an executive action to shut down the loading operations and prevent further liquid inflow. In addition, the process shutdown and isolation of all potential energy sources will prevent ignition of flammable gas cloud and potential escalation of hazardous event i.e. fire / explosion. This is considered as a renewable hazard [53] and the system can be restored to the original status upon repair of the tank and associated pipework.

Where the vapour cloud finds an ignition source in the absence of F&G initiation (e.g. failure or delay in detection of flammable atmosphere) it results in fire or explosion event. If immediately

ignited the fire scenarios envisaged are predominantly pool fire because of tank rupture and substantial sudden loss of containment. The pool fire will not be contained within the dedicated bund area as the integrity of the bund is diminished which may affect adjacent facilities. In the case of a delayed ignition, the consequence of release may be a Vapour Cloud Explosion (VCE) for onshore assets with potential for generating high overpressure magnitude depending on the level of confinement and congestion of the area. Due to the severity of the consequence associated with fire or explosion, they are considered as non-renewable fatal hazardous events and hence are excluded from the proposed Markov model in this paper. Other initiating causes that could lead to over pressurisation of the tank such as exposure of the LST to external fire leading to Boiling Liquid Expanding Vapour Explosion (BLEVE) are excluded from this analysis. A list of foreseeable Hazardous Events (HEs) and associated consequences upon imposition of process demand on PRVs taking into account the available mitigating IPLs is listed in Table 7. The $HE_1$ represents the outcome of PRVs being operational whereas $HE_2$ – $HE_4$ correspond to consequences of PRV failure on demand studied in this paper. The hazardous event $HE_5$ is excluded from the scope of this study due to the severity of the consequence as the system restoration to the original operating state is not deemed as feasible in a timely manner.

Table 7 – Hazardous Events & Consequence Descriptions

| Event | Description | Hazardous Event |
|---|---|---|
| $HE_1$ | Disposal of excess fluid via flare, no Loss of Containment (LoC) | repeatable |
| $HE_2$ | LoC, contained within the bund and drained | renewable |
| $HE_3$ | LoC outwith the bund, detected by gas detection system | renewable |
| $HE_4$ | LoC outwith the bund, undetected gas release, unignited cloud | renewable |
| $HE_5$ | Ignited HC release, fire / explosion with substantial asset damage | non-renewable fatal |

## 5.4 Analysis of Pressure Protection System

The bowtie diagram in Figure 11 presents the Basic Events (BEs) and protection layers in which their failures generate demand on LST pressure relief valves.

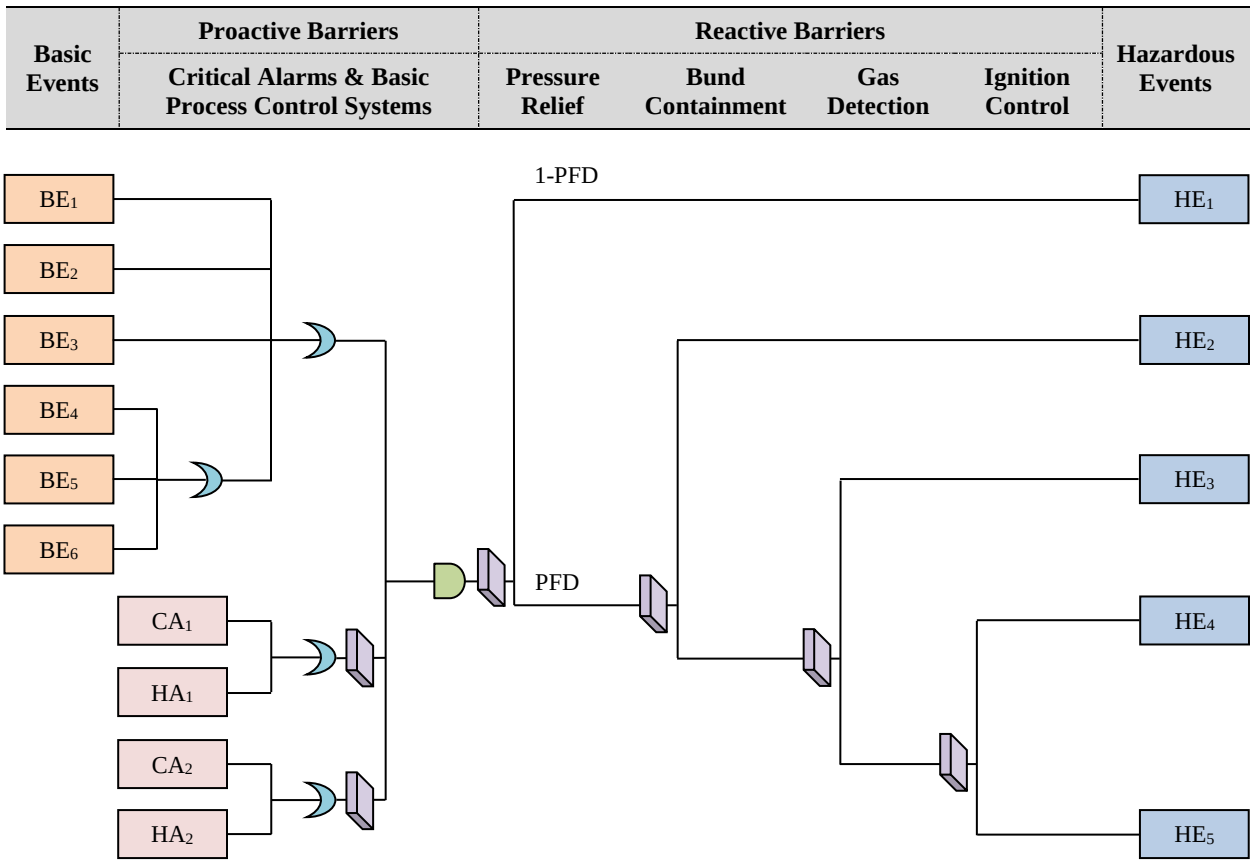


Figure 11 – Process Hazard Analysis Using Bowtie Methodology

The reliability data for instrumentation in Table 8 is extracted from the PDS Data Handbook [52] for individual components. The reliability figures for equipment are obtained in accordance with the Offshore Reliability Data (OREDA) project [56]. In line with the IEC 61508 [4] recommended value, the MTTR value for all equipment / instrumentation is set at 8 hours. The proof test interval is determined based on maintenance and operability requirements of the equipment accordingly. The FIC subsystem is considered as an industrial Programmable Logic Controller (PLC) comprised of an analogue input, a single processing unit (CPU) and a digital output configuration. The failure rate of the Flow Control Valve (FCV) is specified for frequently operated service. The failure rates associated with FCV actuators, pilot / solenoid valve etc. are excluded from this analysis.

Table 8 – Initiating Causes & Failure Frequencies

| Event | Initiating Cause | $\lambda_{DU}(\times 10^{-6}/h)$ | $MTTR(h)$ | $\tau(h)$ |
|---|---|---|---|---|
| $BE_1$ | Isolation Valve ($V_3$) Fails Closed | 2.1 | 8 | 17,520 |
| $BE_2$ | Pump (PZ) Failure to Start | 2.5 | 8 | 8,760 |
| $BE_3$ | Isolation Valve ($V_4$) Fails Closed | 2.1 | 8 | 17,520 |
| $BE_4$ | Flow Transmitter (FT) Failure | 0.6 | 8 | 26,280 |
| $BE_5$ | Flow Controller (FIC) Failure | 4.9 | 8 | 4,380 |
| $BE_6$ | Control Valve (FCV) Fails Closed | 2.2 | 8 | 17,520 |

The proactive barriers in this case study are combination of critical alarms (level and pressure) and operator action to cease loading operation. The DU failure rate value for the PAH / LAH alarms assumes operating in a clean medium with no potential for clogging of sensing lines [52]. The likelihood of human error is computed in this paper using the Human Error Assessment & Reduction Technique (HEART) technique [57] introduced in 1985. The generic task for this case study considered as "restore or shift a system to original or new state following procedures, with some checking" with nominal human unreliability of 0.003 and an error producing condition of "a mismatch between perceived and real risk" corresponding to a factor of 4 [57]. The likelihood of operator failing to respond to the alarm is therefore calculated as $1.2 \times 10^{-2}$ for the Human Actions (HA) associated with the critical alarms, $HA_1$ and $HA_2$.

Table 9 – Proactive Barrier Failure Frequencies

| Event | Initiating Cause | $\lambda_{DU}(\times 10^{-6}/h)$ | $MTTR(h)$ | $\tau(h)$ |
|---|---|---|---|---|
| $CA_1$ | Level Alarm (LAH) Failure | 0.6 | 8 | 26,280 |
| $CA_2$ | Pressure Alarm (PAH) Failure | 2.0 | 8 | 13,140 |

Using Bowtie methodology in Figure 11, the likelihood of LST discharge line breakdown together with failure of proactive IPLs (pressure and level alarms) leading to uncontrolled rise of the liquid level within LST is estimated as $4.28 \times 10^{-5}$. The tank is loaded every 6 hours via trucks, hence the loading frequency can be computed as 0.17 per hour assuming continuous operation within a year (i.e. 8,760h). Therefore, the frequency of process demand imposition on PRVs considering the loading frequency and probability of failure for LST discharge line is obtained as $\lambda_{DE} = 7.13 \times 10^{-6}$. The process demand duration is assumed to be $\mu_{DE} = 1 \times 10^{-4}$ per hour. The restoration rate from hazardous event is also projected as $\mu_T = 1 \times 10^{-3}$ per hour

[19] corresponding to 1000h mean restoration time after a hazardous event takes place. This estimate is deemed as suitable since we are addressing repeatable and/or renewable hazardous event only, although the severity of the consequence dominates this value.

## 5.5 Reliability Performance of Protection System

### 5.5.1 Analysis of Overall Model

The PDS Handbook [52] provides the following additional estimates for the PRV failures rates: $\lambda_{DD} = 0$, $\lambda_D = \lambda_{DU} = 2.2 \times 10^{-6}$ per hour and $\lambda_S = 1.1 \times 10^{-6}$ per hour. Moreover, we set the mean repair time of a safe failure as 10h corresponding to $\mu_S = 1 \times 10^{-1}$ per hour. The CCF factor ($\beta_U$) varies between 0.01 and 0.2 as per IEC 61508 recommended range hence an average value of $\beta_U = 0.1$ is applied. The interval between proof tests is also considered to be two years or $\tau = 17{,}520$h. These estimates are uncertain and will be strongly dependent on the maintenance regime of the LST facilities. The SRS reliability data are summarised in Table 10.

Table 10 – SRS Reliability Data

| **SRS** | $(\times \mathbf{10^{-6}}/\boldsymbol{h})$ | | | $(\times \mathbf{10^{-4}}/\boldsymbol{h})$ | | | | | $(\boldsymbol{h})$ | |
|---|---|---|---|---|---|---|---|---|---|---|
| | $\boldsymbol{\lambda_S}$ | $\boldsymbol{\lambda_{DD}}$ | $\boldsymbol{\lambda_{DU}}$ | $\boldsymbol{\mu_S}$ | $\boldsymbol{\mu_{DD}}$ | $\boldsymbol{\mu_{DU}^{1oo1}}$ | $\boldsymbol{\mu_{DU}^{1oo2}}$ | $\boldsymbol{\mu_{CC}}$ | $\boldsymbol{MTTR}$ | $\boldsymbol{\tau}$ |
| PRV | 1.1 | 0 | 2.2 | 1000 | 0 | 1.14 | 1.71 | 1.14 | 8 | 17,520 |

The DU repair rate for single and redundant SRS systems are calculated as per Equations (16) and (22) respectively. The state equations were solved using MATLAB for both 1oo1 and 1oo2 systems presented in this paper and the calculated PFD and HEF values are outlined in Table 11:

Table 11 – Reliability Analysis Results for 1oo1 & 1oo2 SRSs

| **Performance Indicator** | **PFD** | **HEF** |
|---|---|---|
| 1oo1 SRS | $1.67 \times 10^{-2}$ (SIL 1) | $2.60 \times 10^{-7}$ |
| 1oo2 SRS | $1.93 \times 10^{-3}$ (SIL 2) | $3.13 \times 10^{-8}$ |

As shown a 1oo1 SRS achieves SIL 1 target only whereas introduction of a redundant element improves reliability of the system by an order of magnitude meeting SIL 2 requirements. The system response to the variation in CCF factor (0.01 – 0.2) is also analysed in Figure 12 where 1oo1 simple system remains stagnant whereas the PFD for 1oo2 configuration increases as the $\beta_U$ value rises but remains substantially lower than a 1oo1 system. The behaviour of the 1oo2

model is further studied in Figure 13 which illustrates that the redundant configuration can achieve both SIL 2 and SIL 3 depending on the value of CCF factor. This highlights the prominence of $\beta_U$ and appropriate design method to reduce its impact on functionality of SRSs.

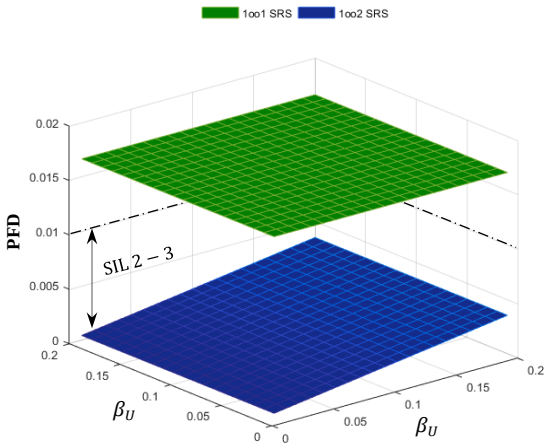


Figure 12 – PFD comparison of 1oo1 SRS vs 1oo2 SRS with varying $\beta_U$ value

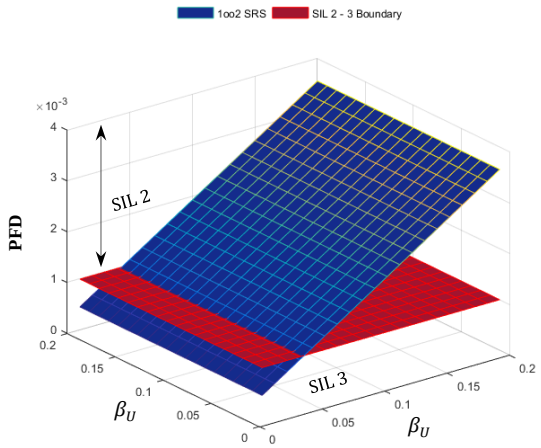


Figure 13 – PFD trend for 1oo2 SRS with varying $\beta_U$ value

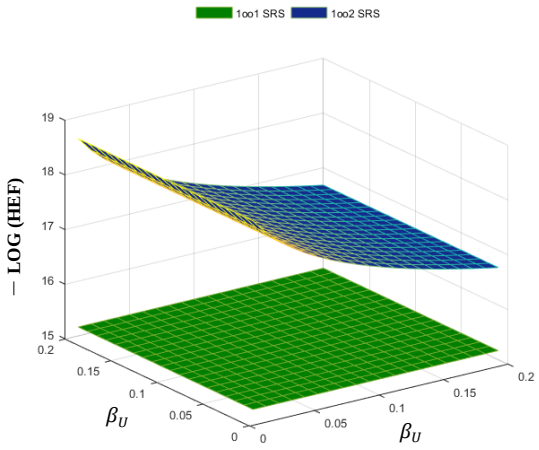


Figure 14 – HEF comparison of 1oo1 SRS vs 1oo2 SRS with varying $\beta_U$ value

The safety performance of the system for 1oo2 SRS is also enhanced due to reduction in hazardous event frequency in comparison with a simple configuration. The graphical representation of this improvement is shown in Figure 14. The reduction in HEF is more apparent for lower values of CCF factor but declines as the $\beta_U$ acquires higher values although it remain lower than the simple system in its entirety. The model behaviour with respect to variation in CCF factor is coherent with the general features of redundant configurations.

### 5.5.2 Comparison of Markov Model vs IEC 61508 Approach

A comparison of performance indicators for the proposed Markov model versus IEC 61508 approach to compute the PFD of 1oo2 SRS is carried out. Despite the PFD trends against variation in CCF factor is identical for both methods across two SIL ranges (SIL 2 and 3) in Figure 15, the IEC 61508 approach gives more conservative results due to higher PFD. The variation between the results is minimal however a reliability improvement between 9% - 15% can be observed from the corresponding curves acquired with the Markov technique. This is a reaffirmation on accuracy and consistency of the Markov model in the reliability analysis of SRSs which is in line with IEC 61508 [4] average PFD calculation requirements. Although the IEC 61508 approach overlooks the impact of process demand in its computation of average PFD, Markov model considers all influencing elements including demand rate and its duration in addition to established system failure modes and repair rates.

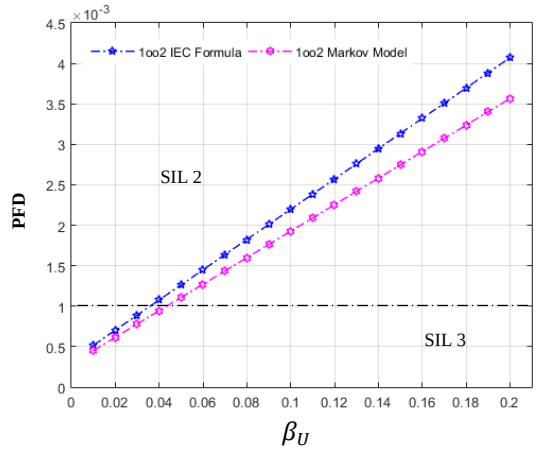


Figure 15 – PFD comparison of Markov Model vs IEC 61508 Approach for 1oo2 SRS with varying $\beta_U$ value

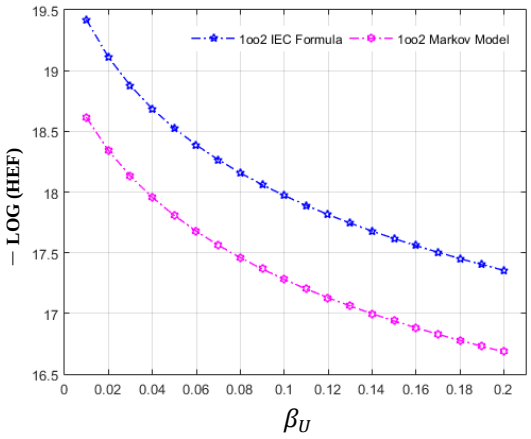


Figure 16 – HEF comparison of Markov Model vs IEC 61508 Approach for 1oo2 SRS with varying $\beta_U$ value

The two methods for calculating the system performance are also compared with regards to HEF and the result is shown in Figure 16. The HEF for both techniques increases as the CCF factor rises, however the IEC 61508 method shows lower frequency of visit to hazardous event when comparing with Markov Model. This reduction can be explained by the supplementary part of HEF equation for 1oo2 Markov model:

Table 12 – HEF Comparison of Markov Model vs IEC 61508 Approach for 1oo2 SRSs

| Technique | Markov Model | IEC 61508 Approach |
|---|---|---|
| 1oo2 SRS | $\lambda_{DE}PFD_{1oo2} + \lambda_{DU}(\beta_U P_4 + P_2)$ | $\lambda_{DE}PFD_{1oo2}$ |

This is due to flexibility of Markov model to evaluate dynamic behaviour of the system taking into cognisance all possible means of system entering hazardous event whereas, the IEC 61508 have no visibility on vulnerability of SRS at the time of response to demand imposition.

### 5.5.3 Impact of Proof Test Interval on Reliability Performance

The behaviour of the proposed 1oo2 SRS model against various proof test intervals, $\tau$, in conjunction with variation in CCF factor, $\beta_U$, is evaluated in this section and the model performance is shown in Figure 17 – Figure 19. The proof test intervals used for illustration purpose vary between 3 years to 1 month periods and the CCF factor alternates between 0.01 and 0.2. It is observed that the reliability performance of the 1oo2 system improves gradually by simultaneous reduction of proof test intervals and CCF factor in Figure 17.

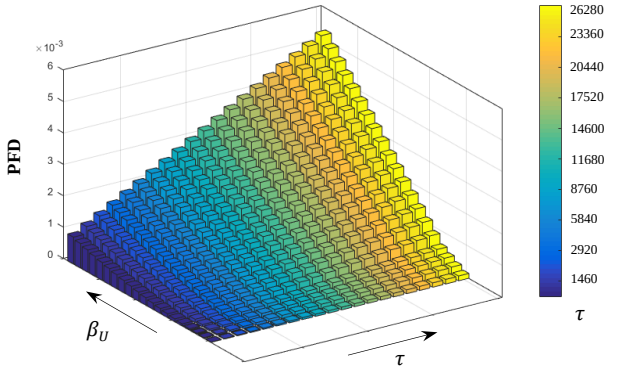


Figure 17 – PFD variations against $\tau$ and $\beta_U$ values for 1oo2 SRS

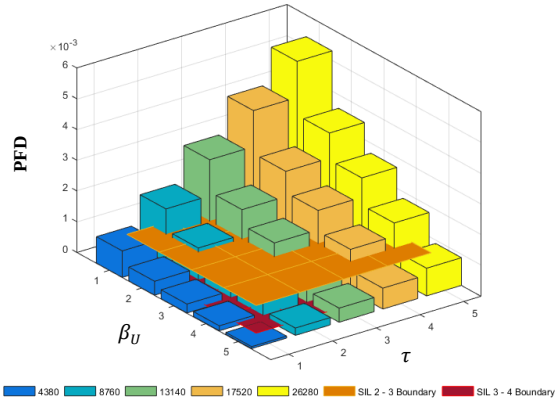


Figure 18 – PFD variations against $\tau$ and $\beta_U$ values for 1oo2 SRS: comparison with SIL boundaries

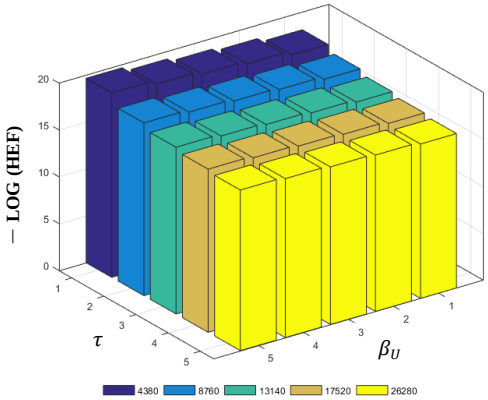


Figure 19 – HEF variations against $\tau$ and $\beta_U$ values for 1oo2 SRS

A selective value set of the abovementioned range as per Table 13 was analysed further together with the boundaries of SIL 2/3 and SIL 3/4 in Figure 18. As shown, a suitable level of safety integrity can be accomplished by optimising the proof test interval and CCF factor. Whilst the combined effect of high proof test interval and upper range CCF factor pushes PFD value towards mid SIL 2, the combined lower values of $\tau$ and $\beta_U$ can be utilised to attain SIL 4 accordingly. The flexibility of fluctuating between SIL 2 - 4 using alternative values, affords an opportunity for the design engineer to adjust the SRS in accordance with the design requirements as deemed appropriate.

Table 13 – Selected Range for Proof Test and CCF Factor

| **Parameters** | **5** | **4** | **3** | **2** | **1** |
|---|---|---|---|---|---|
| $\tau$ | 26,280h | 17,520h | 13,140h | 8,760h | 4,380h |
| $\beta_U$ | 0.01 | 0.05 | 0.1 | 0.15 | 0.2 |

The system visit frequency to hazardous event for the selected range of proof test and CCF factor (Table 13) is illustrated in Figure 19. A decrease in HEF is seen as the proof test interval reduces from 3 years to 1 month although due to logarithmic scale the disparity is deemed as a minimal decline. A reduction in HEF pattern is also perceived as the CCF factor gains lower values. The reduction in HEF is more notable for lower values of proof test and negligible variations are identified as the proof test interval rises. As such, the proof test interval has a more dominant impact on HEF in comparison with the CCF factor. The results can also be used for prioritisation of influencing factors at design stage of the SRS. The above illustration indicates that the proposed 1oo2 safety related system model is in line with the anticipated trend against variations in proof test intervals and CCF factor.

The outcome of this appraisal concludes that reduction in proof test intervals will generally result in reduction of failure on demand probability and system visit to hazardous event simultaneously. However, the implementation of minimum proof test interval may not be practical as other influencing elements play a substantial role in determination of the optimum test interval. The expenditure associated with conducting the proof tests on a more frequent basis including labour / equipment on one hand and disruption in process continuity (e.g. risk associated with shutdown and start-up even though for a limited period) on the other hand will be

dominating factors and may overcome the benefits gained because of reduced proof test interval. As such, a balance between expenditure and maintaining safety integrity of the system is required to be established. A cost benefit analysis to facilitate application of risk reduction to As Low As Reasonably Practicable (ALARP) level would be beneficial in these circumstances.

## 5.6 Sensitivity Examination of 1oo2 SRS

We now investigate the effect of varying model parameters including the demand rate, demand duration, component failure and associated repair rates on the reliability and safety performance of 1oo2 SRS. The effect of varying parameters on the PFD and HEF are evaluated for $\beta_U$ in the range of 0.01 - 0.2 as recommended by IEC 61508.

### 5.6.1 The Effect of $\lambda_{DE}$ and $\mu_{DE}$

We first study the effect of varying the demand rate, $\lambda_{DE}$. The effect of varying $\lambda_{DE}$ on the PFD and HEF are evaluated for demand rates equal to $10^{-8}$, $10^{-7}$, $10^{-6}$, $10^{-5}$ and $10^{-4}$ respectively. In order to illustrate the visit frequency to hazardous event we use -$\log_{10}$ scale on the y-axis. The PFD and HEF are functions of $\lambda_{DE}$ for the specified range of $\beta_U$ value as illustrated in Figure 20 and Figure 21 respectively.

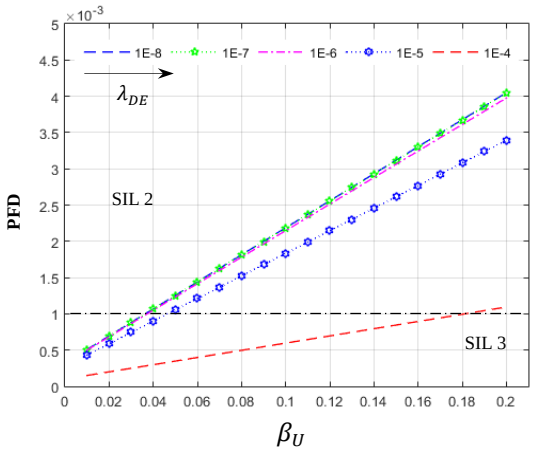


Figure 20 – PFD verses $\beta_U$ with varying $\lambda_{DE}$

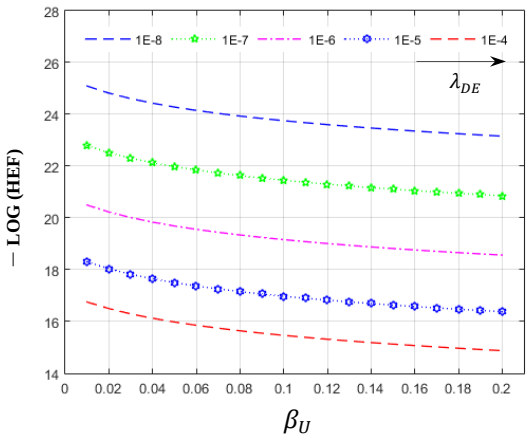


Figure 21 – HEF verses $\beta_U$ with varying $\lambda_{DE}$

Increase in process demand means shifting from low demand mode to high demand mode of operation where SRS is required to respond more frequently to the demands inflicted by the process system. The PFD decreases as the demand rate rises according to the result shown in

Figure 20. This behaviour can be justified considering that the system will respond to the process demand more frequently whilst the demand frequency is on the rise. Therefore, the SRS function is discharged regularly resulting in reduction of test intervals and the system probability of failure on demand due to undetected dangerous failure will naturally reduce, as reflected by reduction in PFD value. Besides, the PFD ascends whilst the CCF rises for various $\lambda_{DE}$ based on Figure 20. The rise in PFD is steeper for lower demand rates however for more frequent process demands, the PFD increases gradually and hence loses sensitivity to the rise in $\beta_U$. The hazardous event frequency ascends whilst $\lambda_{DE}$ obtains higher values for a 1oo2 SRS as per Figure 21. This is due to prevailing impact of $\lambda_{DE}$ in HEF determination ($\lambda_{DE}PFD_{1oo2} + \ldots$), which dictates an increase in HEF despite reduction of PFD. This behaviour was anticipated considering the system is responding more often to process demand and component failures during this period will impair system capabilities in implementing protecting function. The curves for the different demand rates have a similar pattern and increase as the CCF rate elevates.

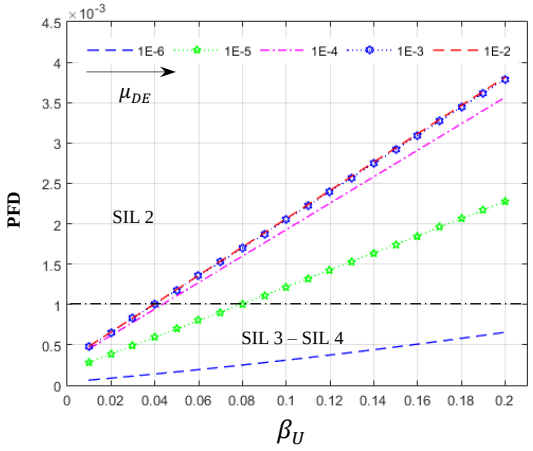


Figure 22 – PFD verses $\beta_U$ with varying $\mu_{DE}$

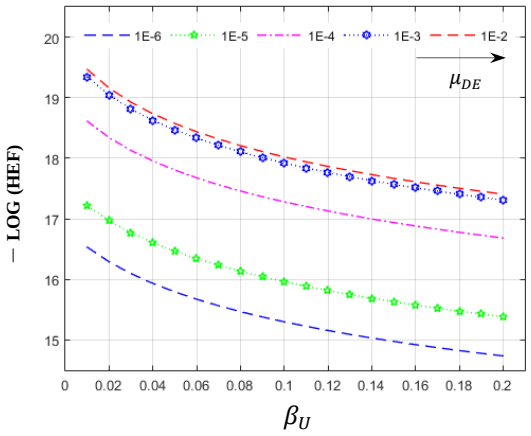


Figure 23 – HEF verses $\beta_U$ with varying $\mu_{DE}$

The effect of varying $\mu_{DE}$ on the PFD and HEF is also assessed for $\beta_U$ in the similar range of 0.01 - 0.2. Calculations are performed for five different values of demand reset rates including $10^{-6}$, $10^{-5}$, $10^{-4}$, $10^{-3}$ and $10^{-2}$ and the results of these variations on the PFD and HEF are illustrated in Figure 22 and Figure 23 respectively. The PFD increases whilst the demand reset rate rises (i.e. demand duration reduces) as seen in Figure 22. This might be predicted by the following argument according to system transition diagram in Figure 7: as the demand duration reduces, the system spends lower portion of time in responding to the process demand in states 4

and 2. As such the likelihood of system transit to the remaining system states including states 1 and 5 increases. This leads to higher system unavailability considering that the PFD for 1oo2 SRS is defined as per Table 4. No disparity in the PFD trend for demand reset rates of $10^{-3}$ and $10^{-2}$ is perceived although an increase in PFD value is observed whilst the CCF rate is on the rise. It is noted that the 1oo2 SRS can achieve SIL 3 / SIL 4 when demand reset rate is set at $10^{-6}$. As the demand duration reduces, the HEF descends in Figure 23 indicating improvement in safety performance for the 1oo2 safety related system. The frequency of system entering hazardous event shows an increase in HEF as the CCF failure rates obtain higher values across all selected values of $\mu_{DE}$. The outcome of this sensitivity investigation is consistent with the observations of Liu et al. [19] for the effect of $\lambda_{DE}$ and $\mu_{DE}$ on a 1oo2 SRS (PRV system) in which the reliability performance indicators PFD and HEF exhibit a similar trend.

### 5.6.2 The Effect of $\lambda_{DU}$, $\mu_{DU}$ and $\mu_{CC}$

In order to study the effect of DU failure rate, $\lambda_{DU}$, on PFD and HEF, the assessment was conducted for various DU failure rates equal to $10^{-8}$, $10^{-7}$, $10^{-6}$, $10^{-5}$ and $10^{-4}$. Increase in component failure rate results in unavailability of SRS to respond to process demand and ultimately a surge in system average PFD as reflected in Figure 24. The PFD for the selected range of $\lambda_{DU}$ ascend sharply as the DU failure rate gains higher values, where $\lambda_{DU} = 10^{-4}$ can no longer achieve SIL target as defined in IEC 61508.

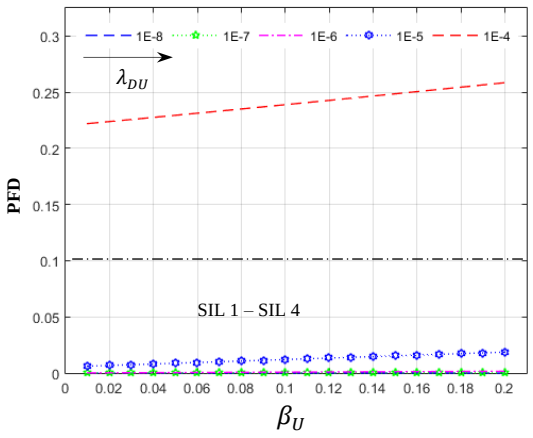


Figure 24 – PFD verses $\beta_U$ with varying $\lambda_{DU}$

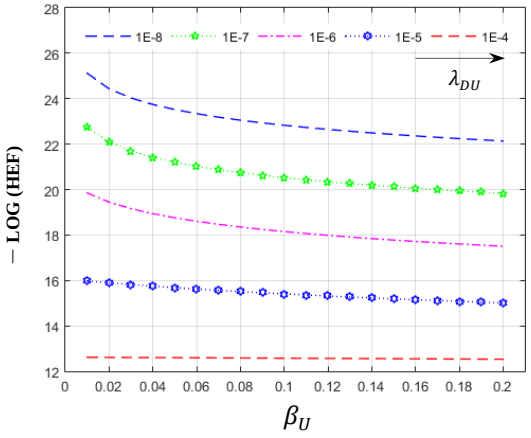


Figure 25 – HEF verses $\beta_U$ with varying $\lambda_{DU}$

This behaviour is also reiterated in the system visit to hazardous event scenario. As observed in Figure 25 the exposure to hazardous event increases since the system components fail more

frequently, reducing system availability to respond to process demand. The hazardous event frequency generally increases as the CCF rate rises for various $\lambda_{DU}$ values however, the impact of $\beta_U$ on HEF is less apparent for higher DU failure frequencies as $\lambda_{DU} = 10^{-4}$ remains constant across the designated values for $\beta_U$. This may be due to the dominant impact of component failure rates that neutralise any change in $\beta_U$ values.

The effect of DU failure rate on the reliability performance of 1oo2 SRS redundant system is in line with 1oo1 simple system. The PFD and the visit frequency of 1oo1 SRS for a low demand system are obtained by $PFD \approx {}^{1}/_{2}\,(\tau.\lambda_{DU})$ and $HEF \approx PFD.\lambda_{DE}$ respectively where the mean duration of the demands is smaller than the test interval [4, 19]. This means any alteration in DU failure rate will directly result in increase or decrease in unavailability of SRS and subsequently variation in visit frequency to the hazardous event. This pattern is consistent with the observation made in Figure 24 and Figure 25 as interpreted above which display a similar pattern of behaviour in 1oo1 and 1oo2 systems.

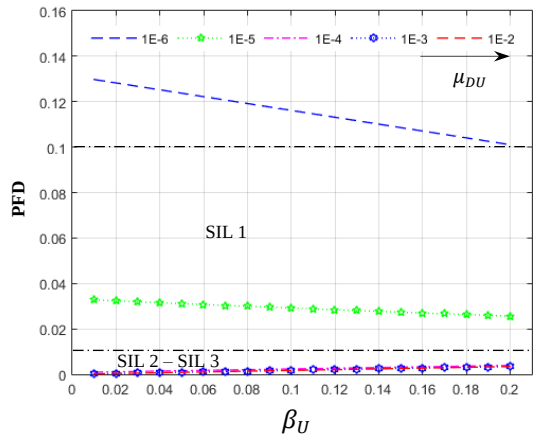


Figure 26 – PFD verses $\beta_U$ with varying $\mu_{DU}$

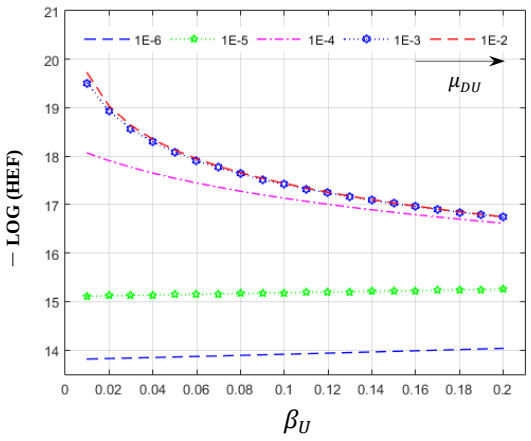


Figure 27 – HEF verses $\beta_U$ with varying $\mu_{DU}$

To explore the impact of DU repair rate, $\mu_{DU}$, on SRS performance indicators, the sensitivity examination was carried out for a diverse range of $\mu_{DU}$ consisting of $10^{-6}$, $10^{-5}$, $10^{-4}$, $10^{-3}$ and $10^{-2}$ consecutively. Higher repair rate leads to increased system reliability and hence is deemed as an improvement in system performance as illustrated in Figure 26 which proves this effect. It is observed that the PFD decreases as DU repair rate increases with $\mu_{DU} = 10^{-6}$ unable to achieve SIL target whereas the DU repair rates of $10^{-4}$, $10^{-3}$ and $10^{-2}$ meet SIL 2 / SIL 3 criteria. The HEF curves demonstrated in Figure 27 against $\beta_U$ for varying DD repair rates show a similar pattern

which is an emphasis on this model behaviour. Due to the enhanced repair rate, the system is less exposed to hazardous event thus a reduction in HEF can be realised in this analysis. Although the HEF increase against variation in $\beta_U$ is more evident for higher values of $\mu_{DU}$, there is no notable change in system visiting the hazardous event when DU repair rate is fluctuating between $10^{-6}$ and $10^{-5}$. The weakest performance of SRS can be identified from Figure 24 – Figure 27 as the combination of high DU failure rate and low DU repair rate which results in a considerable increase in probability of failure on demand for the high pressure protection system and consequently leads to frequent visits to hazardous state. When designing a SRS this combination shall be avoided, otherwise the effectiveness of SRS as an independent layer of protection will be compromised. Conversely the best SRS performance is observed with lowest DU failure rate and highest DU repair rate.

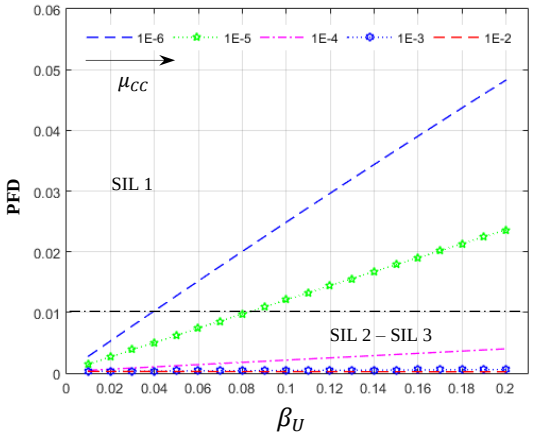


Figure 28 – PFD verses $\beta_U$ with varying $\mu_{CC}$

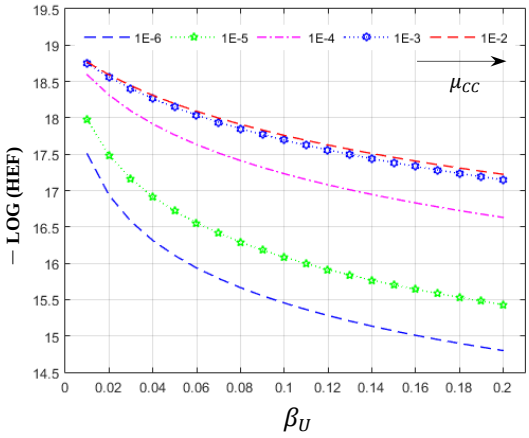


Figure 29 – HEF verses $\beta_U$ with varying $\mu_{CC}$

For completion of the sensitivity analysis, the effect of varying common cause repair rate, $\mu_{CC}$, on the PFD and HEF is also reviewed as part of this study. The sensitivity examination is repeated for $\mu_{CC}$ equivalent to $10^{-6}$, $10^{-5}$, $10^{-4}$, $10^{-3}$ and $10^{-2}$. Consistent with the general philosophy of reliability performance of safety related system, an improvement in PFD is witnessed as the repair rate of common cause failure acquires higher values. It is noted that the PFD reduces as the common cause repair rate rises with system achieving higher integrity level of SIL 3 for $\mu_{CC}$ obtaining $10^{-3}$ and $10^{-2}$. The rise in $\beta_U$ value leads to the deterioration in probability of failure on demand as shown in Figure 28.

This model behaviour is also reflected in the HEF as the frequency of visit to the hazardous event reduces for higher common cause repair frequency. The reduction in HEF is more evident for lower values of common cause repair rates between $10^{-6}$ – $10^{-4}$ but limited disparity is witnessed when $\mu_{CC}$ is fluctuating between $10^{-3}$ and $10^{-2}$. The impact of increase in $\beta_U$ is noticeable, resulting in deterioration of the HEF across all values of common cause repair rate. The system behaviour against change in $\mu_{DU}$ and $\mu_{CC}$ leads to the same pattern of model behaviour considering that the $\mu_{CC}$ will impact only one transition (from state 5 to state 6), whereas variation in $\mu_{DU}$ will influence several transitions including 2 to 4, 1 to 3 and 3 to 6, and thereby its effect on system performance is more notable.

### 5.6.3 The Effect of $\lambda_S$ and $\mu_S$

As discussed the safe failure of the SRS components should not have any impact on the reliability performance of the system. In order to examine this hypothesis a computation was performed for various safe failure rates comprising $10^{-8}$, $10^{-7}$, $10^{-6}$, $10^{-5}$ and $10^{-4}$. According to Figure 30 and Figure 31 the model displays no sensitivity to variation in $\lambda_S$ and as such it is determined that the reliability performance of the system is independent of the safe failure rates. Fluctuation in the repair rate of safe failures should similarly have no effect of the performance indicators of the 1oo2 SRS. As such the calculation was rerun for safe repair rates of $10^{-4}$, $10^{-3}$, $10^{-2}$, $10^{-1}$ and 1 respectively and the effect of change in $\mu_S$ on PFD and HEF is shown in Figure 32 and Figure 33 consecutively. The result is an emphasis that any variation in repair rate of safe failures has no influence on the reliability performance of the model. This demonstrates the consistency of the model with the expected behaviour of 1oo2 redundant safety related system.

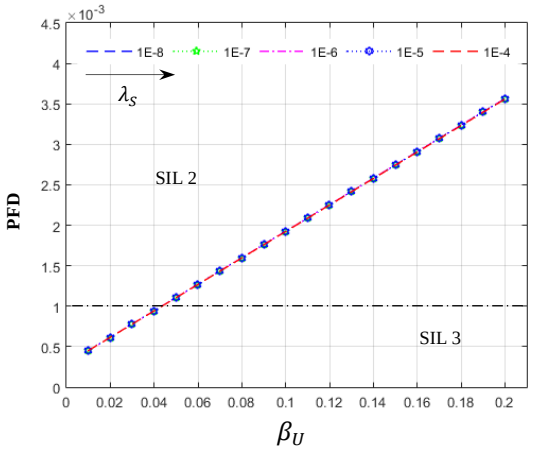


Figure 30 – PFD verses $\beta_U$ with varying $\lambda_S$

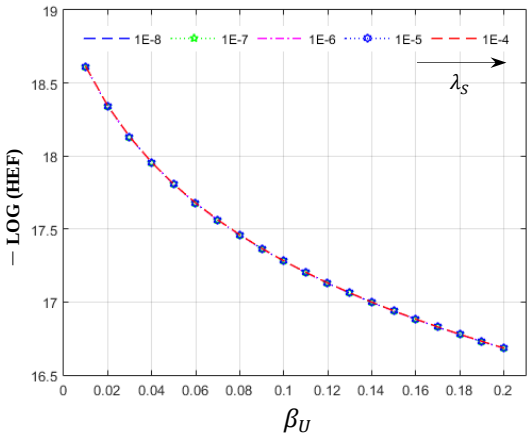


Figure 31 – HEF verses $\beta_U$ with varying $\lambda_S$

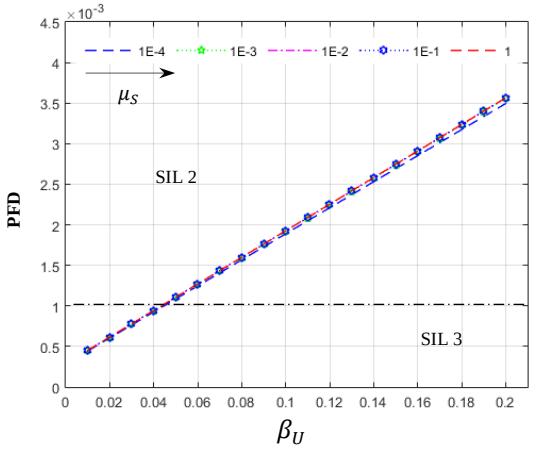


Figure 32 – PFD verses $\beta_U$ with varying $\mu_S$

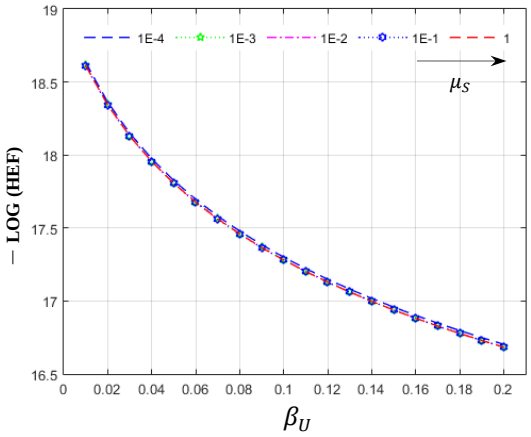


Figure 33 – HEF verses $\beta_U$ with varying $\mu_S$

### 5.6.4 Summary Results

The summary of the sensitivity examination is outlined in Table 14 (excluding safe failure and associated repair) with the specified range of each parameter, PFD upper and lower values and the equivalent safety integrity level the system can achieve.

Table 14 – Sensitivity Examination Summary of PFD & SIL Results for 1oo2 SRS

| Parameter | Range | $\beta_U$ | Lower PFD | High IL | Upper PFD | Low IL |
|---|---|---|---|---|---|---|
| $\lambda_{DE}$ | $10^{-8}$ – $10^{-4}$ | 0.01 – 0.2 | 5.09E-04 | SIL 3 | 1.09E-03 | SIL 2 |
| $\mu_{DE}$ | $10^{-6}$ | 0.01 – 0.2 | 6.35E-05 | SIL 4 | 6.56E-04 | SIL 3 |
| | $10^{-5}$ – $10^{-2}$ | 0.01 – 0.2 | 2.84E-04 | SIL 3 | 3.81E-03 | SIL 2 |
| $\lambda_{DU}$ | $10^{-8}$ | 0.01 – 0.2 | 7.77E-07 | > SIL 4 | 1.54E-05 | SIL 4 |
| | $10^{-7}$ | 0.01 – 0.2 | 8.31E-06 | > SIL 4 | 1.54E-04 | SIL 3 |
| | $10^{-6}$ | 0.01 – 0.2 | 1.36E-04 | SIL 3 | 1.58E-03 | SIL 2 |
| | $10^{-5}$ | 0.01 – 0.2 | 6.10E-03 | SIL 2 | 1.86E-02 | SIL 1 |
| | $10^{-4}$ | 0.01 – 0.2 | 2.22E-01 | < SIL1 | 2.58E-01 | < SIL1 |
| $\mu_{DU}$ | $10^{-6}$ | 0.01 – 0.2 | 1.30E-01 | < SIL1 | 1.01E-01 | < SIL1 |
| | $10^{-5}$ | 0.01 – 0.2 | 3.27E-02 | SIL 1 | 2.56E-02 | SIL 1 |
| | $10^{-4}$ – $10^{-2}$ | 0.01 – 0.2 | 9.59E-04 | SIL 3 | 3.38E-03 | SIL 2 |
| $\mu_{CC}$ | $10^{-6}$ | 0.01 – 0.2 | 2.80E-03 | SIL 2 | 4.83E-02 | SIL 1 |
| | $10^{-5}$ | 0.01 – 0.2 | 1.48E-03 | SIL 2 | 2.36E-02 | SIL 1 |
| | $10^{-4}$ | 0.01 – 0.2 | 4.75E-04 | SIL 3 | 4.00E-03 | SIL 2 |
| | $10^{-3}$ – $10^{-2}$ | 0.01 – 0.2 | 3.04E-04 | SIL 3 | 2.26E-04 | SIL 3 |

No credit has been taken in this case study for safety integrity level below 1 corresponding to $PFD \epsilon [10^{-1}, 0)$. Moreover, the PFD below $10^{-5}$ is considered as exceeding the highest safety integrity level. The results of the sensitivity analysis allow design engineers to identify the contributing parameters to the reliability and safety performance of the system and quantify their impacts. The next step would then be enhancing the system performance utilising positive effects and mitigating the negative impacts of those parameters that compromise the performance of SRSs.

## 5.7 SIL Compliance

There are three separate constraints that must be satisfied in SIL verification to qualify for SIL 2 as per IEC 61508 and IEC 61511. These constraints comprised of PFD Calculation, Hardware Fault Tolerance (HFT) and Systematic Capability (SC). An SRS configuration proposed for SIL 2 application must be based on PFD value, by route 1H or 2H for the architecture constraint, and by systematic capability. If any of these constraints result in a SIL 1 or lower rating, the 1oo2 SRS is not approved for SIL 2 use. The proposed 1oo2 SRS configuration in the paper satisfies the first two constraints and meets at SIL 2 for the 1oo2 configuration. The third requirements in SIL verification process is systematic capability. The proposed configuration can achieve the systematic capability if the SRSs are either SIL 2 certified or the systematic capability can be achieved by "proven in use element" in accordance with IEC 61508. An alternative approach in enhancing the systematic capability is diverse redundancy where the redundant equipment is acquired based on dissimilar design and manufacturing process.

Historically, valve actuators are identified as the weakest point of valve structures due to the complexity of the actuator assembly and required forces to generate adequate momentum in fluid to facilitate closure of the valve. Detailed review of failure records for valves reveals that a large proportion of the failure mechanisms are associated with the valve actuators. In contrast, the PRVs have much simpler structure, do not require signal processing for activation, do not have hydraulic/pneumatic/electric operated actuators and are not required to overcome substantial forces generated by fluids in motion (e.g. emergency shutdown valves) for activation and completion of the safety function. As such large proportion of failure potential associated with

actuators will be eliminated for PRVs. Consequently, the potential for systematic failure is substantially reduced.

The systematic capability is predominantly concerned with considering all potential and unforeseeable scenarios at the design phase that may lead to the failure of SRS (e.g. incorrect selection of material for a temperature element to activate against specific temperature range which is not suitable for the application of interest). In this regard, the systematic capability for simple structure equipment such as PRV is minimal noting the advancement in design and manufacturing processes. Furthermore, the quality management systems associated with fabrication of PRVs are well established within the process industry hence minimising the associated systematic failures. Additionally, the PRVs are usually designed to fail open. Although this results in loss of revenue, commercial losses are the preferred option against other possible consequences (personnel or environmental impact). This is also a contributing factor in reduction of systematic failures since the equipment is designed to fail safe. As such, in the opinion of the authors', the proposed PRV arrangement in Figure 10 is in full compliance with the three distinct requirements of IEC 61508 comprising of PFD Calculation, HFT and systematic capability even though the individual PRV devices have a systematic capability of SIL 1.

# 6.0 Concluding Remarks

In this article, a new reliability model for a redundant safety related system is proposed. The new model for a 1oo2 redundant configuration was developed based on an established 1oo1 simple architecture in low demand mode of operation. The new reliability model uses Markov chains to quantify the uncertainty associated with the probability of failure on demand and frequency of system visit to hazardous event to determine its reliability and safety performance respectively. The process demand imposition on SRS, together with the established system failure modes and associated repairs such as DU failures is considered. Additionally, this model incorporates CCF within the reliability analysis of 1oo2 redundant configuration for the first time. The model presented in this paper is an improvement to the Markov chain previously introduced by Liu et al. [19] by incorporation of CCF rate and associated repair frequency. The new reliability model is proposed for those SRSs where DD failure rate is annulled. The proposed Markov model was

compared with the IEC 61508 approach for 1oo2 redundant safety related system in the same application and its advantages in modelling dynamic behaviour of the systems subject to process demand were observed.

The proposed model in this paper is validated using a case study of pressure protection system for a storage tank facilities handling flammable liquid hydrocarbon. A comparison of 1oo1 simple system versus 1oo2 SRS highlights that the system performance improved predominantly due to the incorporation of a redundant configuration. This verifies that introduction of a redundant element enhances the reliability performance of the system by achieving a higher integrity level as well as improving the safety performance of the system by reducing the frequency of system visiting the hazardous state. The dynamic behaviour of the 1oo2 SRS was further analysed by performing a sensitivity examination of key model parameters including demand rate, demand duration, common cause failure / repair rate and component dangerous undetected failure rates and its associated repair rate. Generally, a deterioration of system performance indicators were witnessed due to the increase in CCF factor as anticipated. The results confirm that the model behaviour against variation in parameters is consistent with the overall expectation of SRS performance for a redundant 1oo2 configuration.

It shall be noted that the assumption with regards to system restoration from the hazardous state to the "as good as new" condition, was made to enable calculation of the steady state probabilities and elimination of absorbing state. In some cases, however, this may not be applicable, or may deem as an unrealistic assumption. From a computational effort prospect, the detailed analysis of a multi-component system (e.g. 2oo3 etc.) will be more complex and the primary aspects of the analysis may easily dissolve in the computational details, however this has not been pursued any further in this paper and may be a topic for further work. At the same time, it would be of great interest to study the effects of DD failure and associated repair rate parameters in a 1oo2 SRS which is subject to process demand as well as inaccuracy of the proof test. These are also new topics for further research. It would also be intriguing to study the effect of homogeneous versus heterogeneous processes and to develop explicit links between constant failure rates and constant transition probabilities (continuous time vs discrete time), in order to explore their impact on the reliability analysis of SRSs. Another area of interest is to compare the

PFD calculation techniques where possible fluctuations (e.g. in process demand) can be captured by Markov modelling but neglected in the international standards formulae.

## Acknowledgments

The authors would like to thank the anonymous reviewers for their constructive comments and feedback.

## Notations

| | |
|---|---|
| $P_i$ | steady state probability for state $i$ |
| $\tau$ | proof test interval |
| $p_{ij}(t)$ | system transition probability from state $i$ to state $j$ |
| $q_{ij}$ | transition rate from state $i$ to state $j$ |
| $\beta$ | total common cause failure factor |
| $\beta_D$ | detected common cause failure factor |
| $\beta_U$ | undetected common cause failure factor |
| $\lambda$ | component failure rate |
| $\lambda_{DE}$ | process demand rate |
| $\lambda_D$ | dangerous failure rate |
| $\lambda_{DD}$ | dangerous detected failure rate |
| $\lambda_{DU}$ | dangerous undetected failure rate |
| $\lambda_S$ | safe failure rate |
| $\lambda_{SD}$ | safe detected failure rate |
| $\lambda_{SU}$ | safe undetected failure rate |
| $\lambda^C$ | common cause failure rate |
| $\lambda^I$ | independent failure rate |
| $\lambda_{DD}^I$ | dangerous detected independent failure rate |
| $\lambda_{DD}^C$ | dangerous detected common cause failure rate |
| $\lambda_{DU}^I$ | dangerous undetected independent failure rate |
| $\lambda_{DU}^C$ | dangerous undetected common cause failure rate |

| | |
|---|---|
| $\lambda_{SD}^{I}$ | safe detected independent failure rate |
| $\lambda_{SD}^{C}$ | safe detected common cause failure rate |
| $\lambda_{SU}^{I}$ | safe undetected independent failure rate |
| $\lambda_{SU}^{C}$ | safe undetected common cause failure rate |
| $\lambda^{T}$ | total failure rate |
| $\mu$ | component repair rate |
| $\mu_{DD}$ | dangerous detected repair rate |
| $\mu_{DE}$ | demand reset rate |
| $\mu_{DU}$ | dangerous undetected repair rate |
| $\mu_{S}$ | safe repair rate |
| $\mu_{T}$ | renewal rate |
| $\pi_i$ | steady state probability of system in state $i$ |
| $DC$ | diagnostic coverage rate |
| $P(t)$ | transition matrix at time $t$ |
| $P_i(t)$ | probability of system in state $i$ at time $t$ |
| $P$ | transition probabilities matrix |
| $r$ | states of stochastic process |
| $f(t)$ | Probability density function of random variable $t$ |
| $F_t(\tau)$ | cumulative distribution function of random variable $t$ for a given $\tau$-value |
| $N(t_k)$ | Number of failures following a Poisson process during time $t$ for component $k$ |

# References


[1] IEC 61511, Functional safety: safety instrumented systems for the process industry sector, parts 1 – 3. Geneva: International Electrotechnical Commission; 2003.

[2] CCPS. Layer of protection analysis; simplified process risk assessment. New York: American Institute of Chemical Engineers, John Wiley & Sons, Inc.; 2001.

[3] Jin H, Lundteigen MA, Rausand M. Reliability performance of safety instrumented systems: A common approach for both low- and high-demand mode of operation. Reliab Eng Syst Saf 2011;96(3):365–73.

[4] IEC 61508, Functional safety of electrical / electronic / programmable electronic safety-

related systems, parts 1 – 7. Geneva: International Electrotechnical Commission; 2010.

[5] IEC 62425, Railway applications – communication, signalling and processing systems – safety related electronic systems for signalling. Geneva: International Electrotechnical Commission; 2007.

[6] ISO/DIS 26262, Road vehicles – functional safety, Parts 1 – 10. Geneva: International Organization for Standardisation; 2009.

[7] Dutuit Y, Innal F, Rauzy A, Signoret JP. Probabilistic assessments in relationship with safety integrity levels by using Fault Trees. Reliab Eng Syst Saf 2008;93(12):1867–76.

[8] Oliveira LF, Abramovitch RN. Extension of ISA TR84.00.02 PFD equations to KooN architectures. Reliab Eng Syst Saf 2010;95(7):707–15.

[9] Yun G, Rogers WJ, Mannan MS. Risk assessment of LNG importation terminals using the Bayesian-LOPA methodology. J Loss Prev Process Ind 2009;22:91–6.

[10] Guo H, Yang X. A simple reliability block diagram method for safety integrity verification. Reliab Eng Syst Saf 2007;92(9):1267–73.

[11] Rausand M, Høyland A. System reliability theory: models, statistical methods, and applications. 2nd ed. New Jersey: Wiley; 2004.

[12] Summers AE. Viewpoint on ISA TR84.0.02 – simplified methods and fault tree analysis. ISA Trans 2000;39(2):125–31.

[13] Misumi Y, Sato Y. Estimation of average hazardous-event-frequency for allocation of safety-integrity levels. Reliab Eng Syst Saf 1999;66(2):135–44.

[14] Bukowski JV, Goble WM. Using Markov models for safety analysis of programmable electronic systems. ISA Trans 1995;34(2):193–8.

[15] Bukowski JV. Incorporating process demand into models for assessment of safety system performance. Proc. RAMS'06 Symp., Alexandria, VI, USA: 2006, p. 577–81.

[16] Langeron Y, Barros A, Grall A, Bérenguer C. Combination of safety integrity levels (SILs): A study of IEC 61508 merging rules. J Loss Prev Process Ind 2008;21(4):437–49.

[17] Rouvroye JL, Brombacher AC. New quantitative safety standards: Different techniques, different results? Reliab Eng Syst Saf 1999;66(2):121–5.

[18] Innal F. Contribution to modelling safety instrumented systems and to assessing their performance Critical analysis of IEC 61508 standard. Ph.D. thesis, University of

Bordeaux, 2008.

[19] Liu YL, Rausand M. Reliability assessment of safety instrumented systems subject to different demand modes. J Loss Prev Process Ind 2011;24(1):49–56.

[20] Alizadeh S, Sriramula S. Unavailability assessment of redundant safety instrumented systems subject to process demand. Reliab Eng Syst Saf 2018; 171: 18-33.

[21] Alizadeh S, Sriramula S. Reliability modelling of redundant safety systems without automatic diagnostics incorporating common cause failures and process demand. ISA Trans 2017; 71(2): 599-614.

[22] Hauge S, Hokstad P, Langseth H, Oien K. Reliability prediction method for safety instrumented systems. Trondheim: SINTEF; 2006.

[23] Wang Y, Rausand M. Reliability analysis of safety-instrumented systems operated in high-demand mode. J Loss Prev Process Ind 2014;32:254–64.

[24] Hokstad P, Corneliussen K. Loss of safety assessment and the IEC 61508 standard. Reliab Eng Syst Saf 2004;83:111–20.

[25] Innal F, Dutuit Y, Rauzy A, Signoret J-P. New insight into the average probability of failure on demand and the probability of dangerous failure per hour of safety instrumented systems. Proc Inst Mech Eng Part O J Risk Reliab 2010;224:75–86.

[26] Jin H, Lundteigen M a., Rausand M. Uncertainty assessment of reliability estimates for safety-instrumented systems. Proc Inst Mech Eng Part O J Risk Reliab 2012;226(6):646–55.

[27] Liu Y, Rausand M. Reliability effects of test strategies on safety-instrumented systems in different demand modes. Reliab Eng Syst Saf 2013;119:235–43.

[28] Marvin Rausand. Risk Assessment: Theory, Methods, and Applications. New Jersey: Wiley; 2011.

[29] Hokstad P. Demand rate and risk reduction for safety instrumented systems. Reliab Eng Syst Saf 2014;127:12–20.

[30] Chebila M, Innal F. Generalized analytical expressions for safety instrumented systems' performance measures: PFDavg and PFH. J Loss Prev Process Ind 2015;34:167–76.

[31] Lundteigen MA, Rausand M. Common cause failures in safety instrumented systems on oil and gas installations: Implementing defense measures through function testing. J Loss

Prev Process Ind 2007;20(3):218–29.

[32] Smith DJ. Reliability, maintainability and risk. 7th ed. Oxford: Butterworth-Heinemann; 2001.

[33] Goble WM, Brombacher AC. Using a failure modes, effects and diagnostic analysis (FMEDA) to measure diagnostic coverage in programmable electronic systems. Reliab Eng Syst Saf 1999;66(2):145–8.

[34] Torres-Echeverría AC, Martorell S, Thompson HA. Modelling and optimization of proof testing policies for safety instrumented systems. Reliab Eng Syst Saf 2009;94:838–54.

[35] Mechri W, Simon C, BenOthman K. Switching Markov chains for a holistic modeling of SIS unavailability. Reliab Eng Syst Saf 2015;133:212–22.

[36] Jin H, Lundteigen MA, Rausand M. New PFH-formulas for k-out-of-n:F-systems. Reliab Eng Syst Saf 2013;111:112–8.

[37] Mechri W, Simon C, BenOthman K, Benrejeb M. Uncertainty evaluation of Safety Instrumented Systems by using Markov chains. Proc. 18th Int. Fed. Autom. Control World Congr., Milano, Italy: 2011, p. 7719–24.

[38] Brissaud F, Barros A, Bérenguer C, Charpentier D. Reliability analysis for new technology-based transmitters. Reliab Eng Syst Saf 2011;96:299–313.

[39] Fleming K. A reliability model for common mode failures in redundant safety systems. Proc. 6th Annu. Pittsburgh Conf. Model. Simul., Pittsburgh, PA, USA: 1974, p. 579 – 581.

[40] Hokstad P, Rausand M. Common cause failure modelling: status and trends. In: Misra KB, editor. Handb. Performability Eng., London: Springer; 2008, p. 621 – 640.

[41] Mechri W, Simon C, BenOthman K. Uncertainty analysis of common cause failure in safety instrumented systems. Proc Inst Mech Eng Part O J Risk Reliab 2011;225(4):450–60.

[42] Barros A, Grall A, Vasseur D. Estimation of common cause failure parameters with periodic tests. Nucl Eng Des 2009;239:761–8.

[43] Vaurio JK. Consistent mapping of common cause failure rates and alpha factors. Reliab Eng Syst Saf 2007;92(5):628–45.

[44] Wierman TE, Rasmuson DM, Mosleh A. Common-cause failure database and analysis

system: event data collection, classification, and coding. Washington, DC: NUREG 6268, U.S. Nuclear Regulatory Commission; 2007.

[45] NEA. Human factor related common cause failure, NEA/CSNI/R(95)10/PART1. NEA/CSNI/. Issy-Les-Moulineaux, France: OECD Nuclear Energy Agency; 1996.

[46] NEA. Compilation of national contributions to a CSNI/PWG1 generic study on human factors related common cause failures, NEA/CSNI/R(95)10/PART2. Issy-Les-Moulineaux: OECD Nuclear Energy Agency; 1996.

[47] Humphreys RA. Assigning numerical value to the beta factor for common cause evaluation. Proc. Reliab. '87, Altrincham, UK: 1987.

[48] Johnston BD. A structured procedure for dependent failure analysis (DFA). Reliab Eng Syst Saf 1987;19:125–36.

[49] Rahimi M, Rausand M. Monitoring human and organizational factors influencing common-cause failures of safety-instrumented system during the operational phase. Reliab Eng Syst Saf 2013;120:10–7.

[50] Zhang T, Long W, Sato Y. Availability of systems with self-diagnostic components – Applying Markov model to IEC 61508-6. Reliab Eng Syst Saf 2003;80(2):133–41.

[51] Mechri W, Simon C, Bicking F, Ben Othman K. Fuzzy multiphase Markov chains to handle uncertainties in safety systems performance assessment. J Loss Prev Process Ind 2013;26:594–604.

[52] Hauge S, Onshus T. Reliability data for safety instrumented systems. Trondheim: SINTEF; 2010.

[53] Yoshimura I, Sato Y. Estimation of calendar-time- and process-operative- time-hazardous-event rates for the assessment of fatal risk. Int J Performability Eng 2009;5(4):377 – 386.

[54] Ouache R, Kabir MN, Adham AAJ. A reliability model for safety instrumented system. Saf Sci 2015;80:264–73.

[55] CCPS. Chemical Process Quantitative Risk Analysis, Hoboken, NJ, USA: American Institute of Chemical Engineers, John Wiley & Sons, Inc.; 2000, p. 1–55.

[56] Langseth H, Haugen K, Sandtorv H. Analysis of OREDA data for maintenance optimisation. Reliab Eng Syst Saf 1998;60:103–10.

[57] Williams JC. HEART – A Proposed Method for Assessing and Reducing Human Error. Proc. 9th Adv. Reliab. Technol. Symp., Bradford, UK: 1986.